

**ONTARIO
SUPERIOR COURT OF JUSTICE**

B E T W E E N:

(Court Seal)

MELISSA MALLETTE

Plaintiff

- and -

BANK OF MONTREAL

Defendant

Proceeding under the Class Proceedings Act, 1992

FRESH AS AMENDED STATEMENT OF CLAIM

TO THE DEFENDANT

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.

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 June 8, 2018 Issued by _____
Amended: September , 2018 Local Registrar

Address of Superior Court of Justice
court office: 161 Elgin Street, 2nd Floor
Ottawa ON K2P 2K1

TO: **Dana M. Peebles**
McCarthy Tétrault LLP
66 Wellington Street West
Suite 5300, TD Bank Tower Box 48
Toronto, ON M5K 1E6

Lawyers for the Defendant, Bank of Montreal

DEFINED TERMS

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

- (a) “**BMO**” means the defendant, Bank of Montreal and, as the context may require, includes its divisions, subsidiaries, partners and affiliates;
- (b) “**CJA**” means the *Courts of Justice Act*, RSO 1990, c C-43, as amended;
- (c) “**Class**” and “**Class Members**” mean all current or former clients of **BMO** whose **Personal Information** was impacted as a result of the **Data Breach**;
- (d) “**Consumer Protection Act**” means the *Consumer Protection Act, 2002*, SO 2002, c 30, Sch A, as amended;
- (e) “**CPA**” means the *Class Proceedings Act, 1992*, SO 1992, c 6, as amended;
- (f) “**Data Breach**” means the unauthorized access to the **Class Members’ Personal Information** through the **Defendant’s** computer systems and networks, which was publicly disclosed by the **Defendant** on May 28, 2018, the events out of which this action arises;
- (g) “**Defendant**” means **BMO**;
- (h) “**Equivalent Consumer Protection Statutes**” means the *Business Practices and Consumer Protection Act*, SBC 2004, c 2, the *Fair Trading Act*, RSA 2000, c F-2, the *Consumer Protection Act*, SS 1996, c C-30.1, the *Consumer Protection and Business Practices Act*, SS 2014, c C-30.2, the *Business Practices Act*, CCSM, c B120, the *Consumer Protection Act*, CQLR, c P-40.1, the *Consumer Protection*

and *Business Practices Act*, SNL 2009, c C-31.1, the *Consumer Protection Act*, RSNS 1989, c 92 and the *Business Practices Act*, RSPEI 1988, c B-7, each as amended;

- (i) **“Personal Information”** means information about an identifiable individual;
- (j) **“PIPEDA”** means the *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5, as amended;
- (k) **“Plaintiff”** means the plaintiff, Melissa Mallette; and
- (l) **“Provincial Privacy Legislation”** means the *Privacy Act*, RSBC 1996, c 373, *The Privacy Act*, CCSM c P125, the *Privacy Act*, RSNL 1990, c P-22, *The Privacy Act*, RSS 1978, c P-24, the *Civil Code of Québec*, CQLR c CCQ-1991, the *Charter of Human Rights and Freedoms*, CQLR c C-12, and the *Act Respecting the Protection of Personal Information in the Private Sector*, RSQ, c P-39.1, each as amended.

CLAIM

- 2. The Plaintiff claims on her own behalf and on behalf of the Class:
 - (a) an order pursuant to the *CPA* certifying this action as a class proceeding and appointing her as a representative plaintiff for the Class;
 - (b) a declaration that the Defendant breached its contracts with the Class Members and that, as a result, the Class Members incurred losses and/or damages;
 - (c) a declaration that the Defendant breached its duty of care to the Class Members and that, as a result, the Class Members incurred losses and/or damages;

- (d) a declaration that the Defendant intentionally or recklessly and without lawful justification invaded the private affairs or concerns of the Class Members in a way that a reasonable person would regard the invasion as highly offensive causing distress, humiliation or anguish;
- (e) with respect to the Class Members who are residents of the Province of British Columbia, a declaration that the Defendant violated section 1 of the *Privacy Act*, RSBC 1996, c 373, as amended;
- (f) with respect to the Class Members who are residents of the Province of Manitoba, a declaration that the Defendant violated section 2 of *The Privacy Act*, CCSM c P125, as amended;
- (g) with respect to the Class Members who are residents of the Province of Newfoundland and Labrador, a declaration that the Defendant violated section 3 of the *Privacy Act*, RSNL 1990, c P-22, as amended;
- (h) with respect to the Class Members who are residents of the Province of Québec, a declaration that the Defendant violated articles 3 and 35-37 of the *Civil Code of Québec*, CQLR c CCQ-1991, section 5 of the *Charter of Human Rights and Freedoms*, CQLR c C-12, and section 10 of the *Act Respecting the Protection of Personal Information in the Private Sector*, RSQ, c P-39.1, each as amended;
- (i) with respect to the Class Members who are residents of the Province of Saskatchewan, a declaration that the Defendant violated section 2 of *The Privacy Act*, RSS 1978, c P-24, as amended;

- (j) an aggregate assessment of damages in the amount of \$500 million or such other amount as may be awarded at trial for:
 - (i) negligence;
 - (ii) breach of contract;
 - (iii) intrusion upon seclusion;
 - (iv) breach of the *Privacy Act*, RSBC 1996, c 373, as amended;
 - (v) breach of *The Privacy Act*, CCSM, c P125, as amended;
 - (vi) breach of *The Privacy Act*, RSS 1978, c P-24, as amended;
 - (vii) breach of the *Privacy Act*, RSNL 1990, c P-22, as amended;
 - (viii) breaches of articles 3 and 35-37 of the *Civil Code of Québec*, CQLR c CCQ-1991, section 5 of the *Charter of Human Rights and Freedoms*, CQLR c C-12, and section 10 of the *Act Respecting the Protection of Personal Information in the Private Sector*, RSQ, c. P-39.1, each as amended;
 - (ix) engaging in unfair practices contrary to and in contravention of Part III of the *Consumer Protection Act* and equivalent provisions in the Equivalent Consumer Protection Statutes; and
- (k) an order pursuant to section 25 of the *CPA* directing individual hearings, inquiries and determinations for members of the Class who have suffered or may have

suffered special damages, including but not limited to identity theft, occasioned by or attributable to the Defendant's breaches as alleged, and all necessary directions relating to the procedures to be followed in conducting hearings, inquiries and determinations;

- (l) aggravated, exemplary or punitive damages in the sum of \$50 million or such other sum as the Court may order;
- (m) prejudgment interest in accordance with section 128 of the *CJA*;
- (n) post-judgment interest;
- (o) an order directing a reference or giving such other directions as may be necessary to determine the issues, if any, not determined at the trial of the common issues;
- (p) the costs of this action plus, the costs of notice and of administering the plan of distribution of the recovery in this action plus applicable taxes; and
- (q) such further and other relief as this Honourable Court may deem just.

THE NATURE OF THIS ACTION

3. This action arises as a result of the Data Breach, which affected sensitive and valuable Personal Information of Class Members.

4. Exploiting known or knowable significant cybersecurity vulnerabilities and deficiencies in the Defendant's computer systems and networks, unauthorized persons were able to carry out the Data Breach and steal the sensitive and valuable Personal Information of Class Members.

5. The Personal Information stolen and compromised in the Data Breach includes extremely sensitive information such as: Class Members' names, dates of birth, social insurance numbers, bank account numbers, credit and/or debit card numbers, email addresses, mailing addresses and phone and/or fax numbers, as well as information regarding the Class Members' occupation, residence, citizenship and relationships, among other information.

6. Subsequently, the stolen Personal Information of 100 BMO client Class Members, including that of the Plaintiff, was posted online and publicly exposed on the internet. The Defendant, however, failed to advise the Plaintiff of the fact that her Personal Information had been exposed online or of the additional risks of identity theft or other abuse arising in the circumstances.

7. The nature, extent and scope of Personal Information the Defendant permitted to be accessed and stolen in the Data Breach is shocking and raises grave privacy and security concerns.

8. The Defendant is entrusted with sensitive and valuable Personal Information of millions of people, including that of the Class Members. The Defendant is responsible contractually and at law to diligently collect, store and manage that information, and to safeguard it against unauthorized use, abuse or theft. It is as such required to establish robust technical and technological capabilities and proper policies, procedures and practices to prevent, timely detect and timely and diligently respond to cybersecurity incidents such as the Data Breach.

9. However, the Defendant failed to comply with its duties. It employed substandard security measures that were inappropriate for the sensitivity of the Class Members' Personal Information or to the nature of its business as a financial institution.

10. The Defendant, furthermore, failed to act diligently and timely to address known or knowable cybersecurity vulnerabilities in its systems. By its inappropriate actions and omissions, and as a result of breaches of its duties, the Defendant exposed the sensitive and valuable Personal Information of its clients in the Data Breach.

11. In the aftermath of the Data Breach, the Defendant has promised to strengthen its security measures, a clear acknowledgment that its security measures in place prior to the Data Breach were insufficient. The Defendant ought to have had in place robust security measures appropriate to the Class Members' Personal Information at all times as reasonably required of it. It is shocking that it did not.

12. The Data Breach has and will have far reaching and significant impact and implications on the Class Members' social and personal lives and their financial affairs, the full extent of which has yet to be determined. This proceeding seeks damages for violation of Class Members' privacy and other general, compensatory and/or consequential damages arising from the Defendant's breaches of its duties to prevent, detect in a timely fashion, and timely and diligently respond to the Data Breach.

THE FACTS

A. The Parties

The Plaintiff

13. The Plaintiff is an individual residing in Ottawa, Ontario, who at the relevant time was a banking client of BMO.

14. The Plaintiff's Personal Information was compromised in or as a result of the Data Breach.

15. The Plaintiff is amongst the approximately 100 BMO clients whose personal information was posted and exposed on the internet subsequent to the Data Breach.

16. On or around May 30, 2018, the Plaintiff was advised by BMO that her debit card had been compromised and needed to be replaced. Subsequently, she was advised by BMO's representatives that her other information, such as her phone number and name, may have also been compromised.

17. However, BMO failed to advise the Plaintiff that, in fact, all her Personal Information such as her name, her social insurance number, her date of birth and her home address, among other information, was posted and exposed to the public on the internet. The Plaintiff learned of this fact when she was contacted by the media and advised by the media that her Personal Information was on the internet and could be seen by anyone.

18. The Plaintiff was shocked to learn that her Personal Information was compromised and accessed by unauthorized third parties as a result of the Data Breach. She was further highly offended to learn that her information was in fact exposed to the public on the internet and, furthermore, that BMO had failed to properly and timely advise her of the situation or the steps she had to take to protect herself against identify theft or other misuse or abuse of her Personal Information.

The Defendant

19. The Defendant, BMO, is a Canadian chartered bank that provides personal and commercial banking and other diversified financial services to its clients through its various business divisions, subsidiaries and affiliates. BMO brands its member companies as BMO Financial Group.

20. BMO provides banking services to its clients pursuant to its client agreements or similar contracts, which are executed and formed at the time a person or entity becomes a client of BMO.

21. BMO collects Personal Information of its clients through the clients and/or third parties as a requirement for the provisions of its services at the time it enters into a contract with the clients. BMO also collects and creates Personal Information on its clients during, in the course of or as a consequence of its relationship with its clients. Some of the Personal Information collected, maintained or managed by BMO is unchangeable in nature, thus it cannot be changed in order to guard against misuse.

22. BMO's head office is located in Montreal, Québec, and its executive office is located in Toronto, Ontario.

B. The Data Breach

23. On May 28, 2018, media outlets reported that BMO had been the subject of the Data Breach.

24. The Class Members' Personal Information stolen and compromised in the Data Breach includes their names, dates of birth, social insurance numbers, bank account numbers, credit/debit card numbers, email addresses, mailing addresses and phone and/or fax numbers, as well as information regarding the Class Members' occupation, residence, citizenship and relationships, among other information.

25. Included in the compromised Personal Information were the Class Members' social insurance numbers ("SIN"). A SIN is a critical piece of information about an individual. The Privacy Commissioner of Canada states that "the SIN is important to privacy protection. It can open the door to your personal information and can put you at risk of fraud and identity theft." Service Canada states that one should "provide your SIN only when you know that it is legally required."

26. On May 28, 2018, BMO issued a statement reporting that it had been the subject of the Data Breach:

TORONTO, May 28, 2018 /CNW/ - On Sunday, May 27, fraudsters contacted BMO claiming that they were in possession of certain personal and financial information for a limited number of customers. We believe they originated the attack from outside the country. We took steps immediately when the incident occurred and we are confident that exposures identified related to customer data have been closed off. We have notified and are working with relevant authorities as we continue to assess the situation. We are proactively contacting those customers that may have been impacted and we will support and stand by them. BMO has strong and robust processes in place to protect customer data and we take customer privacy very seriously. Customers are recommended to monitor their accounts and notify BMO with any suspicious activity.

27. Concurrently, media outlets and Canadian Imperial Bank of Commerce ("CIBC") reported a related cybersecurity incident that implicated Personal Information of certain of the clients of CIBC's direct banking division, Simplii Financial.

28. On or about May 27, 2018, an e-mail purportedly sent by the hackers to media organizations explained the alleged methods used to hack BMO's systems to siphon client information. In general and simplified terms, the e-mail explained that hackers were able to carry out the Data Breach using a known or knowable vulnerability in the Defendant's computer

systems which gave excessive permission to “half-authenticated” accounts. The hackers explained that they used an algorithm to generate client card numbers. Then, they used the vulnerability associated with the “half-authenticated” accounts to reset the Class Members’ security questions and, thereby, accessed the Class Members’ accounts. Through this method, the hackers accessed the Defendant’s systems and inappropriately stole the Class Members’ sensitive Personal Information. The hackers alleged that they automated this process by using high speed scripts and computer proxies to pull massive amounts of customer data quickly.

29. Subsequently, an unidentified person posted a data dump on Pastebin.com containing the stolen Personal Information of 100 BMO client Class Members, which included the Plaintiff’s Personal Information.

30. The Data Breach has had an enormous and far reaching impact on the Class Members, the full extent of which is currently unknown.

31. Among other risks of abuse or misuse of their Personal Information, the Class Members are exposed to the risk of identity theft. The consequences of identity theft can be life-changing. Identity theft can destroy a person’s credit rating. Credit ratings are used to determine if a bank should loan money, grant a mortgage, or issue a credit card. Credit ratings are used by some employers. Landlords use credit ratings to decide whether to rent an apartment. Telephone, utility companies and many other companies also conduct credit checks. Identity theft can ruin lives.

32. Given the nature and scale of the Class Members’ Personal Information stolen in or as a result of the Data Breach, the Data Breach will continue to have a profound impact on the Class Members’ lives and financial affairs.

33. Of note, certain other Canadian banks were also the targets of cyberattacks similar to those that resulted in the Data Breach. On or around June 14, 2018, President and Chief Executive Officer of Royal Bank of Canada (“**RBC**”), Mr. Dave McKay, stated that RBC was a target of apparent cyberattacks similar to those reported by the Defendant but that it was able to defend its systems against those cyberattack.

34. That institutions such as RBC were able to defend their systems and networks against similar cyberattacks is a further indication that the Data Breach would have been preventable and it would not have occurred but for the Defendant’s shortcomings and its breaches of duties, as particularized herein.

C. The Defendant’s Duties to Safeguard the Personal Information, to Prevent the Data Breach and to Timely and Diligently Detect and Respond to It

35. The Data Breach would not have happened but for the Defendant’s breaches of its duties owed to the Class Members to securely and responsibly collect, store and manage their Personal Information, to prevent the Data Breach, and to timely detect and properly respond to the Data Breach.

36. The Defendant’s duties, which it breached, were informed by its client agreements, its privacy policies, its internal policies and procedures, privacy laws of Canada and industry practices.

37. The Defendant’s duties were included expressly or impliedly in its contracts with the Class Members, and also informed the Defendant’s duties at common law, and they required that:

- (a) the Defendant must collect, store and manage the Class Members' Personal Information in accordance with all legislation and regulations governing the collection and disclosure of personal information;
- (b) the Defendant must collect, store and manage the Class Members' Personal Information diligently and in accordance with its established privacy policies;
- (c) the Defendant must treat the Class Members' Personal Information as confidential;
- (d) the Defendant must safeguard the Class Members' Personal Information appropriate to its sensitivity against unauthorized use, disclosure or theft; and
- (e) the Defendant must not disclose the Class Members' Personal Information to anyone without or in excess of their knowledge and informed consent, except in the limited and defined circumstances provided under the contracts and the Defendant's privacy policies.

38. At all relevant times, BMO maintained a Privacy Code applicable to its clients, including the Class Members, which forms part of their contracts with BMO. This document purports to set out BMO's commitment to protecting its clients' Personal Information. Among other things, BMO's Privacy Code states:

Our Commitment to You

BMO Financial Group appreciates the opportunity to help you meet your financial needs. From the day Bank of Montreal was founded in 1817, earning and keeping your trust has been at the very core of our business. We are committed to respecting and protecting the privacy and confidentiality of the Personal Information you have entrusted to us. It is important for you to understand what Personal Information we will collect, how we

will use it, and who may see it.

[...]

1. Accountability

We have strict policies and procedures governing how we deal with your Personal Information. Each and every one of our employees is responsible for respecting and protecting the Personal Information to which the employee has access.

[...]

2. Identifying Purpose

When we collect your Personal Information, we may use or disclose it to:

- verify your identity;
- provide and manage products and services you have requested;
- understand your financial services requirements;
- protect against fraud and manage risk;
- determine suitability of products and services for you;
- better manage your relationship with us;
- determine your eligibility for certain of our products and services, or products or services of others;
- comply with legal or regulatory requirements, or as otherwise permitted by law;
- communicate with you regarding products and services that may be of interest;
- understand our customers and to develop and tailor our products and services, and
- respond to any questions you may have.

If a new purpose for using your Personal Information develops, we will identify that purpose.

3. Consent and Your Choices

When you apply for a new product or service, we obtain your consent to collect, use or disclose your Personal Information for the purposes set out in Principle 2, Identifying Purpose."

[...]

5. Limited Use and Disclosure

We will only use or disclose your Personal Information for the purpose(s) it was collected and as otherwise identified in this Privacy Code.

[...]

8. Safeguards

We use physical, electronic and procedural safeguards to protect against unauthorized use, access, modification, destruction, disclosure, loss or theft of your Personal Information in our custody or control.

[...]

39. Moreover, as an entity that collects, uses or discloses Personal Information in the course of commercial activities carried on in Canada, the Defendant is subject to the *PIPEDA*, including Schedule 1 thereof which required, *inter alia*, the following:

- (a) section 4.1 of Schedule 1 required that the Defendant be responsible and accountable for Personal Information and required the Defendant to implement policies and practices to give effect to the principles concerning the protection of Personal Information;
- (b) section 4.2 of Schedule 1 required that the Defendant identify the purposes for which that information was collected at the time or before Personal Information was collected;

- (c) section 4.3 of Schedule 1 required that the knowledge and consent of the Class Members were required for the collection, use or disclosure of Personal Information and that, the Defendant was required to make a reasonable effort to ensure that the Class Members were advised of the purposes for which Personal Information was collected;
- (d) section 4.3.2 of Schedule 1 required that the Class Members' consent be "meaningful," requiring that "the purposes must be stated in such a manner that the individual can reasonably understand how the information will be used or disclosed";
- (e) sections 4.3.5 and 4.3.8 of Schedule 1 specified that Class Members' reasonable expectations were relevant to obtaining consent, and that the Class Members ought to have been afforded the opportunity, subject to legal or contractual restrictions and reasonable notice, to withdraw consent;
- (f) section 4.5 of Schedule 1 required that the Defendant was not permitted to use or disclose the Class Members' Personal Information for any purposes other than those for which it was collected, except with the Class Members' consent; and
- (g) section 4.7 of Schedule 1 required the Defendant to protect the Class Members' Personal Information by security safeguards appropriate to Personal Information's sensitivity to unauthorized access, disclosure, copying or use.

40. Furthermore, the Defendant's duties and responsibilities, which it breached, were also informed by industry practices.

41. At all material times, the Defendant knew that it was the target of significant cyberattacks which, if not prevented, detected in a timely fashion or properly responded to, would have far reaching implications on its clients. Despite its knowledge of those risks, the Defendant failed to act diligently in accordance with its duties and the standards required of it to prevent, timely detect and properly respond to the Data Breach.

42. The substantial risks arising from cybersecurity threats and the necessity for Canada's financial institutions to regularly review, update and adapt their defence systems to the significant and prevalent cybersecurity risks has been the subject of significant commentary in the past several years.

43. In light of the foregoing considerations and risks that were known to the Defendant, Canadian banks have recognized their responsibility to enhance their defence systems against the increasingly widespread and prevalent cyberattacks. Accordingly, protection of clients' information against theft, misuse or abuse has been acknowledged as Canadian financial institutions' top priority.

44. Indeed, a BMO email sent to its clients following the Data Breach acknowledged: "The safety and security of your BMO accounts is our top priority."

45. As a financial institution that collected, managed and used sensitive Personal Information and banking information, *inter alia*, the Defendant was (and is) required by standards applicable to financial institutions to adopt and implement robust security measures reasonably available.

46. However, as elaborated below, despite the Defendant's promises and representations, it failed to protect the Class Members' Personal Information. By its actions and omissions, and as a

result of the breaches of its duties owed to the Class Members, the Defendant exposed the Class Members' sensitive Personal Information in the Data Breach.

D. The Defendant Breached Its Duties to the Class Members

47. The Defendant violated the foregoing duties imposed upon it contractually and by way of Canada's privacy laws and industry standards to prevent and diligently and timely detect and respond to the Data Breach.

48. The Defendant failed to comply with its duties to prevent the Data Breach. It:

- (a) failed to exercise reasonable care to securely collect, store and manage the Class Members' Personal Information;
- (b) failed to establish proper technological measures, procedures, policies and/or practices to protect the Class Members' Personal Information appropriate to the sensitivity of that information;
- (c) failed to establish technological capabilities to permit appropriately lengthy and complex passwords for its banking clients. BMO limits the banking clients' passwords to no more than 6 alphanumerical characters; it does not permit special characters. BMO's capabilities, procedures and practices in regard to their banking clients' passwords are substandard for a financial institution;
- (d) improperly gave unduly excessive permission to improperly authenticated accounts;

- (e) failed to establish reasonably robust technical and technological capabilities, policies, procedures or practices to safeguard the Class Members' Personal Information against unauthorized access, use or theft;
- (f) failed to regularly audit its security measures and procedures and assess them to ensure they were effective or appropriate, and/or failed to timely address improper or ineffective security technologies, procedures or practices;
- (g) failed to diligently act on and address known or knowable vulnerabilities or deficiencies in its computer systems and security measures;
- (h) by and as a result of its actions and omissions, enabled the Data Breach; and/or
- (i) disclosed the Class Members' Personal Information to unauthorized persons, or caused it to be disclosed to unauthorized persons, without the Class Members' knowledge or consent.

49. In the aftermath of the Data Breach, the Defendant has promised to strengthen its security measures with respect to its banking clients. This is an acknowledgement that the Defendant's security measures in place before the Data Breach were inappropriate or insufficient in the circumstances.

50. Moreover, the Defendant breached its duties to adopt, implement and enforce proper policies and practices to timely detect the Data Breach.

51. Furthermore, the Defendant breached its duties to diligently and responsibly respond to the Data Breach. The Defendant failed to establish robust security measures in a timely fashion

following the Data Breach, and it failed to advise the Class Members of the theft of their Personal Information in a timely fashion.

E. The Defendant Intruded upon the Class Members' Privacy Intentionally, Willfully or Recklessly and in a Highly Offensive Manner

52. The Defendant intruded upon the Class Members' privacy intentionally, wilfully or recklessly through and as a result of the following:

- (a) it failed to adopt, maintain and/or enforce proper policies, practices and/or procedures to securely collect, store and manage the Class Members' Personal Information;
- (b) it failed to adopt, maintain and/or enforce proper policies, practices and/or procedures to ensure the safety of Personal Information and protect it against theft by unauthorized third parties;
- (c) it failed to adopt, maintain and/or enforce proper policies, practices and/or procedures to regularly assess the effectiveness and propriety of its security measures on an ongoing basis appropriate to the nature and sensitivity of Personal Information;
- (d) it failed to adopt, maintain and/or enforce proper policies, practices and/or procedures to regularly assess the effectiveness and propriety of its security measures on an ongoing basis appropriate for entities conducting business in Canada's financial sector;

- (e) it failed to adopt, maintain and/or enforce proper policies, practices and/or procedures to properly and diligently audit its computer systems and networks to identify attempts by unauthorized third parties to breach its systems;
- (f) it failed to adopt, maintain and/or enforce proper policies, practices and/or procedures to diligently respond to and address known or knowable cybersecurity vulnerabilities and security deficiencies in its computer systems or networks to prevent the Data Breach;
- (g) it failed to adopt, maintain and/or enforce proper policies, practices and/or procedures to ensure that the Class Members' Personal Information was not disclosed to unauthorized third parties without or in excess of authorization;
- (h) it failed to adopt, maintain and/or enforce proper policies, practices and/or procedures to timely detect the Data Breach;
- (i) it failed to adopt, maintain and/or enforce proper policies, practices and/or procedures to diligently respond to the Data Breach by failing to establish enhanced security measures in a timely fashion following the Data Breach; and/or
- (j) it failed to adopt, maintain and/or enforce proper policies, practices and/or procedures to diligently respond to the Data Breach by failing to advise the Class Members of the Data Breach within an appropriate timeframe following the Data Breach.

53. The Defendant's intrusion upon the Class Members' privacy was highly offensive in light of the following:

- (a) the Defendant was entrusted by the Class Members with their sensitive and valuable Personal Information. However, despite and contrary to its promises, representations and undertakings contractually and otherwise, the Defendant failed to take appropriate steps reasonably required of it to safeguard the Class Members' Personal Information;
- (b) by failing to properly secure the Class Members' Personal Information in a manner appropriate to its sensitivity and the nature of the Defendant's business, the Defendant demonstrated a disregard and disrespect for the Class Members' privacy rights and their interest in safeguarding the integrity of their Personal Information;
- (c) by failing to properly and diligently act upon known or knowable cybersecurity vulnerabilities and security deficiencies to prevent the Data Breach, the Defendant demonstrated a disregard and disrespect for the Class Members' privacy rights and their interest in safeguarding the integrity of their Personal Information;
- (d) the scope of the Data Breach; and/or
- (e) the nature and sensitivity of Personal Information compromised and stolen in and as a result of the Data Breach.

RIGHTS OF ACTION

54. The Plaintiff incorporates herein, repeats and pleads the factual pleadings advanced above, including with respect to the Defendant's duties owed to the Class Members and its breaches of those duties.

A. Negligence

55. On behalf of herself and the other Class Members, the Plaintiff pleads negligence *simpliciter*.

56. The Defendant owed a duty of care to each Class Member to responsibly and securely collect, store and manage their Personal Information and to safeguard it against the Data Breach.

57. The Defendant's duty of care was informed by its contractual obligations, its stated privacy policies and internal policies, *PIPEDA*, Provincial Privacy Legislation and industry standards and practices.

58. The Defendant has admitted and acknowledged that it was responsible for securing and protecting Personal Information of its client Class Members and of its other banking clients.

59. The Defendant stresses the importance of its clients' privacy in its privacy policies. BMO's privacy policy states that it is "committed to respecting and protecting the privacy and confidentiality of the Personal Information" entrusted to it by clients.

60. At all material times, the Class Members were known to the Defendant. It was reasonably foreseeable to the Defendant that the Class Members would suffer losses or damages should the Defendant breach its duty of care to them.

61. The Defendant breached its duty of care owed to the Class Members to responsibly and securely collect, store and manage their Personal Information and to safeguard it against the Data Breach.

62. As a result of the Defendant's breaches of its duty of care, the Class Members have and will continue to suffer foreseeable losses and/or damages, for which the Defendant is liable.

B. Breach of Contract

63. On behalf of herself and the other Class Members, the Plaintiff pleads breach of contract.

64. The Defendant breached its contractual obligations to securely and responsibly collect, store, manage and use the Class Members' Personal Information and to protect that information against unauthorized use, sharing, loss and theft in the Data Breach.

65. As a result of the Defendant's breaches of its contracts with the Class Members, the Class Members have and will continue to suffer foreseeable losses and/or damages, for which the Defendant is liable.

66. The Class Members' contracts with the Defendant are contracts of adhesion and subject to the doctrine of *contra proferentem*.

C. Tort of Intrusion Upon Seclusion

67. On behalf of herself and the other Class Members, the Plaintiff pleads the tort of intrusion upon seclusion.

68. The Defendant invaded, without lawful justification, the Class Members' private affairs or concerns.

69. The Defendant's conduct was intentional or reckless.

70. A reasonable person would regard the invasion as highly offensive, causing distress, humiliation or anguish.

D. Breach of Provincial Privacy Legislation

Residents of the Province of British Columbia

71. On behalf of the Class Members resident in the Province of British Columbia, the Plaintiff pleads that the Defendant violated section 1 of the *Privacy Act*, RSBC 1996, c 373, as amended.

72. The Defendant wilfully and without a claim of right violated the privacy of the Class Members who are residents of the Province of British Columbia.

Residents of the Province of Manitoba

73. On behalf of the Class Members resident in the Province of Manitoba, the Plaintiff pleads that the Defendant violated section 2 of *The Privacy Act*, CCSM c P125, as amended.

74. The Defendant substantially, unreasonably and without claim of right violated the privacy of the Class Members who are residents of the Province of Manitoba.

75. The Plaintiff pleads and relies on section 4 of *The Privacy Act*, CCSM c P125, as amended, with respect to damages.

Residents of the Province of Newfoundland and Labrador

76. On behalf of the Class Members resident in the Province of Newfoundland and Labrador, the Plaintiff pleads that the Defendant violated section 3 of the *Privacy Act*, RSNL 1990, c P-22, as amended.

77. The Defendant wilfully and without a claim of right violated the privacy of the Class Members who are residents of the Province of Newfoundland and Labrador.

Residents of the Province of Québec

78. On behalf of the Class Members resident in the Province of Québec, the Plaintiff pleads that the Defendant violated articles 3 and 35-37 of the *Civil Code of Québec*, CQLR c CCQ-1991, section 5 of the *Charter of Human Rights and Freedoms*, CQLR c C-12, and section 10 of the *Act Respecting the Protection of Personal Information in the Private Sector*, R.S.Q., c. P-39.1, each as amended.

79. The Defendant violated these Class Members' right to respect for their private lives and their right to privacy without their consent and without being authorized by law.

Residents of the Province of Saskatchewan

80. On behalf of the Class Members resident in the Province of Saskatchewan, the Plaintiff pleads that the Defendant violated section 2 of *The Privacy Act*, RSS 1978, c P-24, as amended.

81. The Defendant wilfully and without claim of a right violated the privacy of the Class Members who are residents of the Province of Saskatchewan.

E. Breach of Consumer Protection Legislation

82. The Defendant engaged in unfair practices by making false, misleading or deceptive representations to the Class Members, contrary to the *Consumer Protection Act* the Equivalent Consumer Protection Statutes.

83. The defendant represented to consumers that it maintained strict security safeguards when storing personal information in order to prevent unauthorized access, as described above. In fact, the defendant failed to maintain appropriate or adequate security measures in storing personal information. Contrary to the *Consumer Protection Act* and Equivalent Consumer Protection Statutes, the defendant made false, misleading or deceptive representations that its services had strict security standards that they did not have.

84. By making false, misleading or deceptive representations, the defendant engaged in unfair practices, contrary to the *Consumer Protection Act* and Equivalent Consumer Protection Statutes. Consumers affected by the Contractual Claims are entitled to rescind their contracts and/or an award of damages pursuant to the *Consumer Protection Act* and Equivalent Consumer Protection Statutes.

85. By this claim, Class Members hereby give notice pursuant to s. 18(3) of the *Consumer Protection Act* (and pursuant to any parallel provisions of the Equivalent Consumer Protection Statutes). In the alternative, it is not in the interests of justice to require that notice be given pursuant to section 18(15) of the *Consumer Protection Act* (and pursuant to any parallel provisions of the Equivalent Consumer Protection Statutes). The plaintiff requests an order waiving any such notice requirements.

Damages

86. As particularized herein, the Defendant's actions and omissions constitute intentional, wilful or reckless intrusions upon seclusion and corresponding breaches of its duties at law and contractually owed to the Class Members. The Defendant's actions and omissions resulting in the Data Breach are highly offensive to a reasonable person.

87. The circumstances give rise to serious and far reaching consequences on the Class Members' personal lives and financial affairs the full extent of which has yet to be determined.

88. The Class Members are exposed to a significant risk of identity theft or other misuse or abuse of their Personal Information. The Class Members are furthermore exposed to losses or damages with respect to their finances. Significant time and expenses have and will be required to address the consequences of the Data Breach, and to safeguard the Class Members against identify theft and other misuse or abuse of their Personal Information.

89. The Plaintiff's damages claim represents general, compensatory and consequential damages for:

- (a) general damages to be assessed in the aggregate;
- (b) intrusion upon seclusion;
- (c) loss of privacy;
- (d) loss of valuable Personal Information;
- (e) damage resulting from synthetic or fictitious identity fraud schemes;
- (f) damage to credit ratings and perceived credit worthiness;
- (g) damage to reputation;
- (h) costs and expenses incurred or required to protect the Class Members against identity theft or other misuse or abuse of their Personal Information; and
- (i) lost or wasted time and inconvenience in responding to the Data Breach.

90. Additionally, for and on behalf of each Class Member who as a result of the Data Breach has been the subject of unauthorized withdrawal of funds from his, her or its accounts, whether held by the Defendant or any other bank or financial institution, the Plaintiff claims compensatory damages in the sum that equals the amount of the funds withdrawn from the account without authorization, plus interest calculated at an annual rate to be determined at trial.

91. Moreover, for and on behalf of each Class Member who has suffered further loss and/or damage as a result of the Data Breach, the Plaintiff claims corresponding compensatory damages to be determined, if necessary, at an individual issues trial.

92. Furthermore, on behalf of himself and the Class, the Plaintiff claims aggravated, exemplary or punitive damages in the sum of \$50 million or such other sum as the Court may order. The Defendant's conduct was high-handed, outrageous, reckless, wanton, entirely without care, deliberate, callous, disgraceful, wilful, in contemptuous disregard of the rights of the Plaintiff and other Class Members, and as such renders the Defendant liable to pay aggravated, exemplary and punitive damages.

93. In the circumstances, a significant award of damages is appropriate to mark the wrongs that have been done. The Plaintiff's claim for damages is proper and just in light of:

- (a) the nature, incidence and occasion of the Defendant's wrongful actions and omissions, which failed to prevent or diligently or timely detect or respond to the Data Breach;
- (b) the contractual relationship between the Class Members and the Defendant as well as privacy laws of Canada, which required that the Defendant respect and protect

the Class Members' Personal Information, to securely and responsibly collect, store, and manage that information, and to safeguard it against the Data Breach; and/or

- (c) the conduct of the Defendant both prior to and after the Data Breach.

Vicarious Liability

94. BMO is vicariously liable for the actions and omissions of its subsidiaries, affiliates, partners, directors, officers and employees.

Real and Substantial Connection with Ontario

95. The Plaintiff pleads that this action and each Class Member's claims have a real and substantial connection with Ontario because, among other things:

- (a) The Defendant is resident in Ontario;
- (b) The Defendant carries on business in Ontario;
- (c) Contracts relating to the subject matter of this action were made in Ontario;
- (d) The tort of intrusion upon seclusion was committed in Ontario;
- (e) The Class Members' Personal Information was collected, stored and transmitted in and through Ontario; and
- (f) A substantial portion of the Class Members reside in Ontario.

Relevant Legislation

96. The Plaintiff pleads and relies on the *CJA*, the *CPA*, the *PIPEDA*, the Provincial Privacy Legislation, the *Consumer Protection Act* and the Equivalent Consumer Protection Statutes, each as amended.

Place of Trial

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

(Date of issue)

SOTOS LLP

180 Dundas Street West
Suite 1200
Toronto ON M5G 1Z8

Jean-Marc Leclerc (LSO # 43974F)

Sabrina Callaway (LSO # 65387O)

Tel: 416-977-0007

Fax: 416-977-0717

SISKINDS LLP

Suite 302, 100 Lombard Street
Toronto, ON M5C 1M3

Michael G. Robb (LSO #: 45787G)

Sajjad Nematollahi (LSO #: 62311B)

Tel: 416-594-4390

Fax: 416-594-4391

JSS Barristers

800, 304 - 8 Avenue SW
Calgary, Alberta T2P 1C2

Carsten Jensen, QC

Sean Carrie

Tel: 403-571-1520

Fax: 403-571-1528

Lawyers for the Plaintiff

BANK OF MONTREAL
Defendant

Court File No. CV-18-00076745-00CP

**ONTARIO
SUPERIOR COURT OF JUSTICE**

PROCEEDING COMMENCED AT OTTAWA

Proceeding under the *Class Proceedings Act, 1992*

FRESH AS AMENDED STATEMENT OF CLAIM

SOTOS LLP
180 Dundas Street West,
Suite 1200
Toronto ON M5G 1Z8

SISKINDS LLP
Suite 302, 100 Lombard Street
Toronto, ON M5C 1M3

JSS Barristers
800, 304 - 8 Avenue SW
Calgary, Alberta T2P 1C2

Jean-Marc Leclerc
(LSO # 43974F)
Sabrina Callaway
(LSO # 65387O)

Michael G. Robb (LSO # 45787G)
Sajjad Nematollahi (LSO # 62311B)

Carsten Jensen, QC
Sean Carrie

Tel: 416-977-0007
Fax: 416-977-0717

Tel: 416-594-4390
Fax: 416-594-4391

Tel: 403-571-1520
Fax: 403-571-1528

Lawyers for the Plaintiff