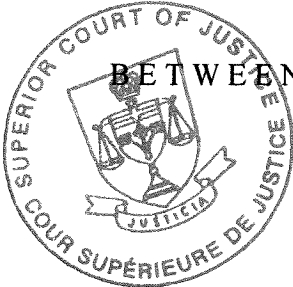


Court File No.: CV-18-00599875-00CP

**ONTARIO  
SUPERIOR COURT OF JUSTICE**



**BETWEEN:**

**JEFF STEINMAN**

**Plaintiff**

**- and -**

**CANADIAN IMPERIAL BANK OF COMMERCE**

**Defendant**

*Proceeding under the Class Proceedings Act, 1992*

**STATEMENT OF CLAIM**

**TO THE DEFENDANT**

A LEGAL PROCEEDING HAS BEEN COMMENCED AGAINST YOU by the plaintiffs. The claim made against you is set out in the statement of claim served with this notice of action.

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 plaintiffs' lawyer or, where the plaintiffs do not have a lawyer, serve it on the plaintiffs, and file it, with proof of service, in this court office, **WITHIN TWENTY DAYS** after this notice of action 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,

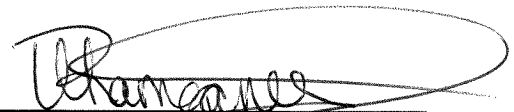
LEGAL AID MAY BE AVAILABLE TO YOU BY CONTACTING A LOCAL LEGAL AID OFFICE.

IF YOU PAY THE PLAINTIFF'S CLAIM, and \$5,000 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 plaintiffs' 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: June 15, 2018

Issued by

  
Local Registrar

Address of court office 393 University Ave. - 10th Fl.  
Toronto ON M5G 1E6

**TO:** Canadian Imperial Bank of Commerce  
Commerce Court  
Toronto, Ontario M5L 1A2

## DEFINED TERMS

1. In this document, in addition to the terms that are defined elsewhere herein, the following definitions apply:
  - (a) “**CIBC**” means the defendant, Canadian Imperial Bank of Commerce and, as the context may require, includes its divisions, subsidiaries, partners and affiliates;
  - (b) “**CIBC Simplii**” means Simplii Financial, the direct banking division of the defendant, **CIBC**;
  - (c) “**CJA**” means the *Courts of Justice Act*, RSO 1990, c C-43, as amended;
  - (d) “**Class**” and “**Class Members**” mean all clients of **CIBC Simplii** whose **Personal Information** was breached in or as a result of the **Data Breach**;
  - (e) “**CPA**” means the *Class Proceedings Act, 1992*, SO 1992, c 6, as amended;
  - (f) “**Data Breach**” means the unauthorized access to and disclosure of the **Class Members’ Personal Information** across and through the facilities of 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 **CIBC**;
  - (h) “**Personal Information**” means 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;
  - (j) “**Plaintiff**” means the plaintiff, Jeff Steinman; and
  - (k) “**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, and the *Charter of Human Rights and Freedoms*, CQLR c C-12, each as amended.

### CLAIM

2. The Plaintiff claims:

- (a) An order certifying this action as a class proceeding under section 5(1) of the *CPA* and appointing the Plaintiff as the representative plaintiff for the Class;
- (b) A declaration that the Defendant breached its contracts with the Class Members, or any of them 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, or any of them 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, or any of them, 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 in the alternative to paragraph 2(d), above, 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 in the alternative to paragraph 2(d), above, 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 in the alternative to paragraph 2(d), above, that the Defendant violated section 3 of the *Privacy Act*, RSNL 1990, c P-22, as amended;
- (h) With respect to the Class Members, if any, who are residents of the Province of Québec, a declaration in the alternative to paragraph 2(d), above, that the Defendant violated articles 3 and 35-37 of the *Civil Code of Québec*, CQLR c CCQ-1991, as amended, and section 5 of the *Charter of Human Rights and Freedoms*, CQLR c C-12, as amended;
- (i) With respect to the Class Members who are residents of the Province of Saskatchewan, a declaration in the alternative to paragraph 2(d), above, that the Defendant violated section 2 of the *Privacy Act*, RSS 1978, c P-24, as amended;
- (j) General, compensatory and/or consequential damages in and for breach of contract, negligence *simpliciter*, intrusion upon seclusion and/or violation of the Provincial Privacy Legislation as follows:
  - (i) For and on behalf of each Class Member, general, compensatory and/or consequential damages in the sum of \$4,760 for intrusion upon seclusion, loss of privacy, loss of valuable Personal Information, lost time and inconvenience in responding to the Data Breach and/or costs or expenses incurred or required to protect them against identity theft or other misuse or abuse of their Personal Information, including to purchase credit monitoring services for the duration of 7 years and, where possible, to

request new social insurance numbers;

- (ii) 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, compensatory damages in the sum that equals the amount of the funds withdrawn from the account without authorization, plus interest for the duration of the time that the funds were missing from the account calculated at an annual interest rate of 22.97%;
- (iii) For and on behalf of each Class Member who has suffered further loss and/or damage as a result of the Data Breach, compensatory damages to be determined, if necessary, at an individual issues trial;
- (k) Aggravated, exemplary or punitive damages in the sum of \$20 million or such other sum as the Court may order;
- (l) 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;
- (m) Prejudgment and post-judgment interest;
- (n) Costs of this action plus, pursuant to s 26(9) of the *CPA*, the costs of notice and of administering the plan of distribution of the recovery in this action plus applicable taxes; and
- (o) Such further and other relief as this Honourable Court may deem just.

## OVERVIEW

3. On May 28, 2018, Canadian media outlets and the Defendant disclosed one of the largest known cybersecurity breaches involving Canadian financial institutions to date.
4. Exploiting known or knowable significant cybersecurity vulnerabilities and deficiencies in the Defendant's computer systems and networks, unauthorized persons were able to breach the Defendant's computer systems and networks. They accessed and stole the sensitive and valuable Personal Information of 40,000 Class Members who were banking clients of CIBC Simplii.
5. Personal Information stolen and compromised in the Data Breach includes essentially all the information the Defendant collected from its client Class Members, namely: Class Members' 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.
6. 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.
7. It has since been revealed that the Data Breach was carried out by exploiting cybersecurity vulnerabilities and deficiencies in the Defendant's computer systems and networks that were known or knowable for several weeks or months prior to the Data Breach. The Defendant, however, failed to diligently address those vulnerabilities and deficiencies in accordance with and appropriate to the standards required of it.
8. A related data breach incident apparently carried out using similar methods and exploiting the same cybersecurity vulnerabilities and deficiencies in the computer

systems and networks of Bank of Montreal (“BMO”) affected Personal Information of up to 50,000 of BMO clients.

9. As one of Canada’s largest national chartered banks, in the course of its commercial for-profit activities, 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.
10. The Defendant operates in Canada’s highly sensitive financial sector, which has been recognized for years to be vulnerable to cybersecurity threats. 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.
11. Indeed, the Defendant has acknowledged its duty owed to its banking clients, including the Class Members, to treat the safety of their Personal Information as a “top priority.”
12. 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.
13. 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 tens of thousands of its clients in the Data Breach.
14. 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 as one Canada's largest banks. It is shocking that it did not.

15. 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

16. The Plaintiff, Jeff Steinman, is a Project Manager residing in Kitchener, Ontario, and a client with CIBC Simplii. Mr. Steinman's Personal Information was stolen in or as a result of the Data Breach.
17. On Saturday, May 26, 2018, Mr. Steinman learned that he had lost access to his online banking account with CIBC Simplii. Mr. Steinman contacted CIBC Simplii's client care representatives, however, the customer care representatives did not advise him that the Data Breach had occurred and his Personal Information had been stolen. Mr. Steinman learned of the Data Breach on Monday, May 28, 2018, when it was disclosed in media reports.
18. Mr. Steinman later identified multiple Interac email transfer attempts in his bank account,

and learned that several hundreds of dollars had been withdrawn from his bank account without authorization. After Mr. Steinman notified CIBC Simplii of the irregular and improper activities in his account, CIBC Simplii froze Mr. Steinman's account and replaced his bank cards. On Tuesday, May 29, 2018, CIBC Simplii refunded Mr. Steinman the principal amount of the funds withdrawn from his account without authorization.

19. Mr. Steinman was shocked and highly offended to learn of the Data Breach, that unauthorized persons had accessed his bank account and transferred the funds out of his account without authorization. Mr. Steinman was further highly offended when he realized that CIBC Simplii's client care representatives did not advise him of the Data Breach and that his Personal Information had been stolen, and that he had to first learn of the Data Breach through media reports several days after his account had been accessed by unauthorized third parties.
20. Mr. Steinman is gravely concerned about his privacy and intends to take steps to ensure the safety of his financial information. In addition to the loss of his valuable Personal Information and the violation of his privacy, the Plaintiff has and will spend many hours, and has and will undergo great inconvenience and incur significant costs to address the Data Breach.

#### The Defendant

21. The Defendant, CIBC, 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.
22. In August 2017, CIBC announced the launch of CIBC Simplii pursuant to a plan to wind

down its President's Choice Financial branded consumer banking offer with Loblaw Companies Limited. Effective November 1, 2017, the clients with President's Choice Financial products transitioned to CIBC Simplii.

23. CIBC Simplii is a division of CIBC. Owned and operated by CIBC, CIBC Simplii provides direct banking services by telephone, online or through a mobile device. CIBC Simplii's banking services and products are provided by CIBC.
24. CIBC provides banking services to CIBC Simplii 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 the CIBC-owned and operated CIBC Simplii.
25. CIBC collects Personal Information of CIBC Simplii 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.
26. CIBC also collects and creates Personal Information on CIBC Simplii clients during, in the course of or as a consequence of its relationship with the clients, including: the number and nature of CIBC Simplii and/or other CIBC accounts held by each client; the value of those accounts and the changes in value of those accounts over time; the number and value of mortgages or loans held by CIBC Simplii clients; the type and value of investment products held by CIBC Simplii or CIBC clients; and the numbers assigned to, or other means of identifying, each client's accounts.
27. A majority of the Personal Information collected, maintained or managed by CIBC is unchangeable in nature, insofar as it relates to characteristics of each CIBC Simplii client that are inherent to that client. Consequently, in most circumstances, the Personal Information cannot be changed in order to guard against misuse.

28. CIBC is one of Canada's largest banks. For the year ended October 31, 2017, CIBC reported revenue in excess of \$16 billion, and net income (profit) of \$4.7 billion. CIBC's registered and head office is located in Toronto, Ontario.

**B) The Data Breach**

29. On the morning of May 28, 2018, media outlets reported that CIBC Simplii had been the subject of a cybersecurity incident affecting its banking clients. The media reports were accompanied by statements from CIBC, reporting that unauthorized persons had breached its computer systems and networks and stolen Personal Information of as many as 40,000 of its client Class Members.
30. Shortly thereafter, it was revealed that the cybersecurity attacks resulting in the Data Breach were undertaken by foreign hackers exploiting known or knowable vulnerabilities and deficiencies in the Defendant's computer and security systems.
31. 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.
32. According to CIBC Simplii in a statement posted on its website on or about May 28, 2018, "On Sunday [May 27, 2018] we received a claim that fraudsters electronically accessed certain personal and account information for some of our clients."
33. On May 28, 2018, CIBC Simplii furthermore posted a statement from its Senior Vice-President, Michael Martin, on its social media platforms, as follows:

Dear Simplii Financial client:

We have implemented enhanced online security measures in response to a claim received on Sunday, May 27 that fraudsters may have electronically accessed certain personal and account information for some of our clients.

In addition to the steps that Simplii has taken, we recommend that clients:

- Always use a complex password and pin (eg. not 12345)
- Monitor their accounts for signs of unusual activity

Clients who notice suspicious activity are encouraged to contact Simplii Financial. If a client is a victim of fraud because of this issue, we will return 100% of the money lost from the affected bank account.

We take this matter seriously and will be reaching out individually to clients who may be impacted. Updated information will be posted here as it becomes available.

Michael Martin, SVP Simplii Financial

34. Concurrently, media outlets and Bank of Montreal reported a related cybersecurity incident that implicated Personal Information of 50,000 clients of Bank of Montreal.
35. Persons apparently responsible for the Data Breach alleged that they were able to breach the Defendant's computer systems and networks by exploiting several known or readily identifiable cybersecurity vulnerabilities and deficiencies in the Defendant's computer systems and online banking security measures.
36. These persons further alleged that the cybersecurity vulnerabilities and deficiencies were known or knowable to the Defendant for several weeks or months prior to the Data Breach. The Defendant, however, failed to properly, diligently or timely address those vulnerabilities and deficiencies, thereby exposing Personal Information of the Class Members.

37. An email dated May 27, 2018, partially disclosed by media outlets, which is attributed to the persons who carried out the Data Breach reads (typographical and grammatical errors in the original):

In the last few weeks, Simplii Financial has been showing Email & SMS spam alert on both their home page and their login page asking their customer to be carefull and as of May 27, 2018, they as showing "Scheduled maintenance". Why ?

There is no simple explanation for that except that Simplii Financial prefer to take their time to analyze the situation instead of actually protecting their customer information. The vulnerability of Simplii Financial is based on the same concept than the BMO vulnerability using LUHN algorithm to generate card number then accessing their information from the vulnerability.

The BMO vulnerability has been half patched a first time in January 2018. This vulnerability left over 50,000 customer information in our hands (Card Number, Security Question, Account Balance, Account Number, All transactions available in online banking, Name, Address, Phone Number (Home,Business,Fax), Employment Info, Social Insurance Number, Date of Birth, and more).

To make this vulnerability possible you had to exploit the way BMO used cookie to authenticate their user. They were giving too much permission to half-authenticated account which enabled us to grab all these information. By half authenticated account I mean the BMO was not checking if a password was valid until the security question were input correctly.

We then made a first software to extract customer data from the database at high speed which they noticed quickly. They have put a small patch online which limited the amount of thread we could use to 2 per server.

We then used over 500 different ip (socks 5 proxy from a private provider) to use in our software in multi-threading over proxy.

The second vulnerability after January 2018 was based on an information leak from BMO. BMO again had given too much permission to half authenticated account. BMO enabled us through their function to create saving goals to gain access to the bank account number of BMOs account which enabled us to

then reset these account password using the bank account number automatically in a new software.

Simplii financial are giving too much permission to half authenticated account too. While Using the password reset function on their website, their are creating a session cookie from the card number you input, that session cookie is used from simplii to access to security question of the account and keep it active for the next step. When sending the generated card number to simplii for password reset, simplii will ask us the 3 security question in order to reset. . We don't have them (But we are half authenticated) So we simply have to access the Security Question reset link that we would normally under a fully authenticated user to reset them. Wait ? We now have the 3 security questions !!!

We go to the same password reset function a second time, enter the generated card number, enter the 3 security question we just reset from the vulnerability and now we have access to the account

But that's not all. Both Simplii Financial and BMO are shutting down the case. They know their customer security is was and will be at risk!

-BMO still does have a small vulnerability as of May 07 2018. They still allow their customer account to be access without security questions using a fully authenticated account and a half authenticated account.

-We have more than 50,000 BMO users information with all the information stated above.

38. The Data Breach has had an enormous and far reaching impact on the Class Members, the full extent of which is currently unknown.
39. In the aftermath of the Data Breach, Class Members have reported similar experiences with their online banking and accounts. They have reported that their bank accounts had been improperly accessed, funds had been stolen or otherwise transferred out of their bank accounts, their passwords and/or security questions had been changed and, generally, they were locked out of their online banking accounts.
40. Many Class Members have reported that they first learned of the unusual activities

concerning their accounts when they were trying to complete a transaction using their debit or credit cards and the transaction was rejected due to the suspension of the debit or credit cards or a substantial decrease in their spending limits.

41. Many Class Members have reported that they have spent several hours with the Defendant's client care representatives and others (including their service providers or business partners) to learn what had happened and/or otherwise address the situation, including to request a refund of the funds withdrawn from their accounts without authorization and to replace their debit and/or credit cards and banking information.
42. Furthermore, many Class Members have reported that, when they contacted the Defendant's client care centres upon observing unusual activities in their bank accounts, they were not initially advised by the Defendant's representatives of the Data Breach. Instead of advising such Class Members of the Data Breach and ensuring that proper steps were taken to safeguard their Personal Information and banking information, the Defendant's client care representatives simply directed such Class Members to reset their passwords, a measure that would not have been effective in safeguarding the Class Members' online banking or Personal Information in the circumstances.
43. Many Class Members have reported that they first learned of the Data Breach on May 28, 2018, when it was reported by the media or through social media platforms, noting that the Defendant had failed to directly contact them in a timely fashion.
44. Moreover, many Class Members have reported that although they were able to receive a refund for the funds stolen from their bank accounts held with the Defendant, their bank accounts had been cancelled and they were left with no banking solution, a situation that adversely impacted their personal and commercial financing and needs.



45. 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. 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 individual or commercial 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, including to purchase proper credit monitoring for a reasonable period of at least seven years and, where possible, to replace their social insurance numbers.

**C) Cybersecurity Risks and Data Breaches are a Known and Priority Concern for Canadian Banks**

46. 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.
47. 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.
48. For example, in December 2014, Bank of Canada issued a report titled "Cyber Security: Protecting the Resilience of Canada's Financial System," containing the following key highlights:

- (a) “Cyber attacks have the potential to pose systemic risk by disrupting the business operations of key participants in Canada’s financial system”;
- (b) “The operational resilience of these participants—large financial institutions and the financial market infrastructures (FMIs) they participate in—is central to the overall resilience of the financial system”;
- (c) “The attackers targeting elements of Canada’s financial system are a diverse group, with varying levels of sophistication and capabilities”; and
- (d) “Canadian financial institutions and FMIs have been proactive in building up their defences against cyber attacks, and actively collaborate with one another and with the federal government.”

49. In conclusion, the report further noted:

In addition to traditional threats to operational resilience, financial institutions and financial market infrastructures are facing growing challenges in the form of cybersecurity threats. The extensive reliance on technology by financial institutions and financial market infrastructures, coupled with the high degree of interconnectedness between them, increases the sector’s vulnerability to a cyber attack. Hence, both private and public sector stakeholders have recognized the need to work together to address these potential vulnerabilities.

50. Bank of Canada’s Financial System Review, dated June 2017, further highlighted the cybersecurity threats to Canada’s financial system, calling for cybersecurity to be treated as a “public good.” Identifying cyber threats as one of the key vulnerabilities of the Canadian financial system, the report noted:

The financial system’s cyber defences must have the capacity to withstand both internal and external threats, particularly as they relate to the Internet. The increasing incidence and severity of cyber attacks highlight a particular threat to financial institutions. The interconnectedness of the financial system could lead to rapid transmission of stress from a cyber attack. This is a structural vulnerability that is unlikely to go away. And because of the interconnections in the system, the public sector has a role in coordinating cyber defences.

[...]

*Cyber threats are evolving rapidly and require adaptable defences*

The level of sophistication and frequency of cyber attacks have been growing over the past several years as the tools and skills needed to launch an attack have become more widely available. Financial institutions, including central banks, are frequent targets of high-profile cyber attacks. For example, in 2016 alone, at least eight monetary authorities in various jurisdictions were victims of a cyber attack; the most notable incident was the Bangladesh Bank heist, where hackers stole US\$81 million.

51. In light of the foregoing considerations and risks posed by cyber threats, Canadian banks have recognized their responsibility to enhance their defence systems against the increasingly widespread and prevalent cyberattacks.
52. Protection of clients' information against theft, misuse or abuse has been acknowledged as Canadian financial institutions' top priority.
53. Indeed, a CIBC Simplii email sent to its clients following the Data Breach acknowledged: "The safety and security of your Simplii account is our top priority."
54. However, as elaborated below, despite the Defendant's promises and representations, it failed to treat the safety and security of the Class Members' Personal Information as its so-called "top priority." 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's Duties to Safeguard the Personal Information, to Prevent the Data Breach and to Timely and Diligently Detect and Respond to It**

55. 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.

56. 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.
57. 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 in accordance with its sensitivity; 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.
58. At all relevant times, CIBC maintained a Privacy Policy applicable to CIBC Simplii's clients, including the Class Members, detailing how CIBC purported to collect, use, share and protect its clients' Personal Information. Among other things, the CIBC Privacy Policy stated:

At CIBC, we take the protection of your personal information seriously. We make reasonable efforts to prevent unauthorized use, sharing, loss and theft of information. We regularly audit our security procedures and assess that they remain effective and appropriate.

59. Furthermore, at all relevant times, CIBC maintained a document titled CIBC Privacy Principles applicable to CIBC Simplii clients, including the Class Members which, *inter alia*, stated:

CIBC is responsible for personal information under its control.

[...]

CIBC protects the privacy of personal information through security measures appropriate to the sensitivity of the information.

60. 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.
61. Furthermore, the Defendant's duties and responsibilities, which it breached, were informed by industry practices. 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, including but not limited to:
- (a) appropriate technical and technological capabilities to permit strong, lengthy and complex passwords;
  - (b) two factor authentication; and

- (c) suspicious login email notification.

**E) The Defendant Breached Its Duties to the Class Members**

- 62. 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.
- 63. The Defendants failed to comply with their duties to prevent the Data Breach. They:
  - (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. CIBC's capabilities, procedures and practices in regard to their banking clients' passwords are substandard for a financial institution. Of note, CIBC would permit and require more complex and lengthier passwords for access to other parts of their computer systems and networks, including employees' emails. It is questionable and astonishing that it would not permit properly lengthy and complex passwords for access to its banking clients' information;
  - (d) improperly gave unduly excessive permission to "half-authenticated" accounts, a significant vulnerability that allowed unauthorized access to the Class Members' banking accounts and information through and across the Defendant's computer

systems and networks in the Data Breach;

- (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 outdated or otherwise 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; and/or
- (h) by and as a result of its actions and omissions, enabled the Data Breach and caused the Class Members' Personal Information to be disclosed or disclosed Class Members' Personal Information to unauthorized third parties in the Data Breach.

64. 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 admission and acknowledgement that the Defendant's security measures in place before the Data Breach were inappropriate or insufficient in the circumstances.
65. Of note, on or about May 30, 2018, the former Privacy Commissioner of Ontario, Ms. Ann Cavoukian, commented on the Data Breach, expressing the concern that the Defendant should have employed better security measures and practices from the beginning; "I expect [CIBC] to have the highest level of protection possible, and clearly [it] didn't."



66. Moreover, the Defendant breached its duties to adopt, implement and enforce proper policies and practices to timely detect the Data Breach. The Defendant failed to detect the Data Breach on its own in a timely fashion. According to the Defendant, it learned of the Data Breach only after it was contacted by persons who carried out the Data Breach.
67. 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 continues to use substandard and improper security measures for access to its banking clients' information.
68. Furthermore, many Class Members, including the Plaintiff, were not advised by the Defendant of the Data Breach or theft of their Personal Information in a timely manner. Many Class Members, including the Plaintiff, first learned of the Data Breach and/or the theft of their Personal Information through the media, demonstrating the Defendant's shortcomings in properly and timely communicating the Data Breach and the risks arising thereof to the Class Members.

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

69. 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 leaked information that was used in the cyberattacks and resulted in the Data Breach;
- (f) 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;
- (g) 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;
- (h) 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;
- (i) it failed to adopt, maintain and/or enforce proper policies, practices and/or procedures to timely detect the Data Breach;

- (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 establish enhanced security measures in a timely fashion following the Data Breach; and/or
- (k) 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.

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

- (a) 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;
- (b) 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;
- (c) in the circumstances, despite its promises, representations, and undertakings the Defendant has demonstrated that the safety and security of the Class Members' Personal Information has not been a top priority;
- (d) the scope of the Data Breach, which encompassed up to 40,000 of the Defendant's banking clients, making the Data Breach one of the largest

cybersecurity incidents implicating Canadian financial institutions; 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**

- 71. 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) Breach of Contract**

- 72. On behalf of himself and the other Class Members, the Plaintiff pleads breach of contract.
- 73. 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. As a result, the Class Members have and will continue to suffer losses and/or damages.
- 74. The Class Members' contracts with the Defendant are contracts of adhesion and subject to the doctrine of *contra proferentem*.

#### **B) Negligence *Simpliciter***

- 75. On behalf of himself and the other Class Members, the Plaintiff pleads negligence *simpliciter*.
- 76. 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.
- 77. 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.

78. 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.
79. At all material time, 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.
80. 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. As a result of the Defendant's breaches of its duty of care, the Class Members have and will continue to suffer losses and/or damages.

**C) Tort of Intrusion upon Seclusion**

81. On behalf of himself and the other Class Members, the Plaintiff pleads the tort of intrusion upon seclusion.
82. The Defendant invaded, without lawful justification, the Class Members' private affairs or concerns.
83. The Defendant's conduct was intentional or reckless.
84. A reasonable person would regard the invasion as highly offensive, causing distress, humiliation or anguish.

**D) Violation of Provincial Privacy Legislation**

85. In the alternative to the tort of intrusion upon seclusion, the Plaintiff pleads the following

claims for and on behalf of the Class Members resident in the Provinces of British Columbia, Manitoba, Newfoundland and Labrador, Québec and Saskatchewan.

Residents of the Province of British Columbia

86. On behalf of the Class Members resident in the Province of British Columbia, the Plaintiff pleads in the alternative to the tort of intrusion upon seclusion that the Defendant violated section 1 of the *Privacy Act*, RSBC 1996, c 373, as amended.
87. 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

88. On behalf of the Class Members resident in the Province of Manitoba, the Plaintiff pleads in the alternative to the tort of intrusion upon seclusion that the Defendant violated section 2 of the *Privacy Act*, CCSM c P125, as amended.
89. The Defendant substantially, unreasonably and without claim of right violated the privacy of the Class Members who are residents of the Province of Manitoba.
90. 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

91. On behalf of the Class Members resident in the Province of Newfoundland and Labrador, the Plaintiff pleads in the alternative to the tort of intrusion upon seclusion that the Defendant violated section 3 of the *Privacy Act*, RSNL 1990, c P-22, as amended.
92. 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

93. On behalf of the Class Members (if any) resident in the Province of Québec, the Plaintiff pleads in the alternative to the tort of intrusion upon seclusion that the Defendant violated articles 3 and 35-37 of the *Civil Code of Québec*, CQLR c CCQ-1991, as amended, and section 5 of the *Charter of Human Rights and Freedoms*, CQLR c C-12, as amended.
94. 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

95. On behalf of the Class Members resident in the Province of Saskatchewan, the Plaintiff pleads in the alternative to the tort of intrusion upon seclusion that the Defendant violated section 2 of the *Privacy Act*, RSS 1978, c P-24, as amended.
96. The Defendant wilfully and without claim of a right violated the privacy of the Class Members who are residents of the Province of Saskatchewan.

**Damages**

97. On behalf of himself and each other Class Member, the Plaintiff claims general, compensatory and consequential damages in the sum of \$4,760 per Class Member for intrusion upon seclusion, loss of privacy, loss of valuable Personal Information, lost time and inconvenience in responding to the Data Breach and expenses incurred or required to protect them against identity theft or other misuse or abuse of their Personal Information, including to purchase credit monitoring services for the duration of 7 years and, where possible, to request new social insurance numbers.
98. 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 for the duration of the time that the funds were missing from the account calculated at an annual interest rate of 22.97%.

99. Additionally, 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.
100. Additionally, on behalf of himself and the Class, the Plaintiff claims aggravated, exemplary or punitive damages in the sum of \$20 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.
101. This claim for damages is proper and just in the circumstances 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;



- (c) the distress, embarrassment and annoyance suffered by the Class Members as a result of the Data Breach;
- (d) the conduct of the Defendant both prior to and after the Data Breach; and/or
- (e) the impact of the Data Breach on the Class Members' social lives, businesses, and personal and financial affairs.

#### **Vicarious Liability**

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

#### **Real and Substantial Connection with Ontario**

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

- (a) The Defendant is domiciled and 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**

104. The Plaintiff pleads and relies on the *CJA*, the *CPA*, the *PIPEDA* and the Provincial Privacy Legislation, each as amended.

**Place of Trial**

105. The Plaintiff proposes that this action be tried in the City of Toronto, in the Province of Ontario, as a proceeding under the *CPA*.
106. The Plaintiff intends to serve a jury notice.

DATE: June 15, 2018

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

**Michael G. Robb** (LSO #: 45787G)  
Tel: 519-660-7872  
Fax: 519-660-7873

**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**

JEFF STEINMAN  
and  
CANADIAN IMPERIAL BANK OF  
COMMERCE

Plaintiff Defendant

Court File No.: CV - 18-00599875-00CP

ONTARIO  
SUPERIOR COURT OF JUSTICE

Proceeding commenced at Toronto

Proceeding under the *Class Proceedings Act, 1992*

STATEMENT OF CLAIM

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

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

**Michael G. Robb (LSO #:**  
45787G)  
Tel: 519-660-7872  
Fax: 519-660-7873

**Carsten Jensen, QC**  
**Sean Carrie**  
Tel: 403-571-1520  
Fax: 403-571-1528

**Sajjad Nematollahi (LSO #:**  
62311B)  
Tel: 416-594-4390  
Fax: 416-594-4391

Lawyers for the Plaintiff