

Claim No.

05-CV-283484CP

ONTARIO
SUPERIOR COURT OF JUSTICE

BETWEEN:

THEODORE JOEL SPEEVAK

Plaintiff

- and -

CANADIAN IMPERIAL BANK OF COMMERCE

Defendant

Proceeding under the *Class Proceeding Act*, 1992

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.

Date: February 4, 2005

Issued by 
Local Registrar

Address of court office:
393 University Avenue, *10th Floor*
Toronto, Ontario
M5G 1E6

TO: Canadian Imperial Bank of Commerce
25 King Street West
Toronto, ON

CLAIM

1. The plaintiff and the class members claim:
 - (a) an Order pursuant to the *Class Proceedings Act*, S.O. 1992, c. 6, certifying this proceeding as a class proceeding and appointing Theodore Joel Speevak as representative plaintiff;
 - (b) damages for breach of contract in the amount of \$3,000,000.00;
 - (c) in the alternative, damages for breach of the plaintiff's and class member's rights under the *Personal Information Protection and Electronic Documents Act* in the amount of \$3,000,000.00;
 - (d) in the further alternative, damages for breach of duty of care in the amount of \$3,000,000.00;
 - (e) class wide aggravated and exemplary damages in the amount of \$3,000,000.00;
 - (f) class wide punitive damages in the amount of \$3,000,000.00;

- (g) pre-judgment interest pursuant to the provisions of the *Courts of Justice Act*, R.S.O. 1990, c. 43, as amended;
- (h) costs and applicable GST on a substantial indemnity basis; and
- (i) such further and other relief as this Honourable Court shall deem just.

The Parties

2. The plaintiff, Theodore Joel “Ted” Speevak, is an individual who resides in the City of Toronto, in the Province of Ontario. The plaintiff was at all material times a client of the defendant, Canadian Imperial Bank of Commerce (“the bank”).

3. The defendant is a chartered bank incorporated pursuant to the laws of Canada, with its head office in the city of Toronto, in the Province of Ontario. At all material times, the bank provided banking, financial and investment services to its clients, including the plaintiff and the class members.

4. The class members are all persons who were, at the material time, clients of the bank and whose sensitive personal information was disclosed to unauthorized third

parties by bank employees using unsecured facsimile transmission machines, as described in this statement of claim.

The Facts

5. The bank is in the business of, among other things, providing banking, financial and investment services to its clients. The bank also provides its clients with registered investment opportunities.

6. In the course of providing banking, financial and investment services, the bank requires disclosure of private, personal information of the client. Such information typically includes the client's name, address, telephone numbers, social insurance number, bank account numbers, GIC Instrument numbers and amounts, credit card numbers and signature.

7. The information collected by the bank is personal information of the clients as defined in the *Personal Information Protection and Electronic Documents Act* (2000), c. 5. ("PIPEDA")

8. The personal information of the class members is “sensitive” information as that term is described in Section 4.3.4 of Schedule 1 to *PIPEDA*.

9. The bank determined that it would use unsecured facsimile transmission machines to transfer information from its branches to its central operations service group. The bank intended to, and did use this unsecured means of information transfer to send sensitive personal information of its clients, including the class members.

10. In or about 2001, if not earlier, the bank began disclosing sensitive personal information of the class members to third parties. These third parties had no right to receive the sensitive personal information of the class members. The bank had not informed the class members, nor had it obtained consent from the class members to disclose the their sensitive personal information to the third parties.

11. The third parties were involuntary recipients of the sensitive personal information of the class members.

The Bank's First Notification by Allstar

12. One of the third parties was Allstar Sportsline Products Inc. (“Allstar”). In or about 2001, after receiving several facsimiles containing sensitive personal information of class members, Allstar contacted the bank by telephone and advised the bank that it had improperly sent personal client information to Allstar via facsimile transmission.

13. The bank took no steps to address the concerns of Allstar nor to determine the cause of the improper disclosure of sensitive personal information of the class members. The bank took no steps to determine the individuals whose right to privacy had been violated by the bank, nor did it take any steps to notify individuals that their privacy had been violated and warn them of steps to be taken to protect themselves against identity theft or other misuse of their sensitive personal information.

14. Employees of the bank continued to make unsecured facsimile transmissions and continued to send sensitive personal information of class members to third parties after the first notification by Allstar.

The Bank’s Second Notification by a Class Member

15. Allstar became frustrated with the bank’s continued faxing of clients’ sensitive personal information to its offices. On or about February 25, 2002, Allstar contacted

a class member using sensitive personal information contained in one of the further facsimiles it had received from the bank. Allstar advised the class member that the information had been sent to them and described the sensitive nature of the information which had been disclosed by the bank.

16. The class member contacted the local bank manager and reported the significant breach of the class member's privacy and security of sensitive personal information.

17. As a result of the notification by the class member, the bank was aware that its employees were continuing to use the unsecured facsimile transmission lines and that sensitive personal information of clients was continuing to be disclosed to third parties who had no right to receive such information.

18. The bank failed to take any, or, in the alternative, sufficient steps to investigate and to ensure that the breach of its clients' privacy did not reoccur.

19. Following this notification by the class member, the bank took no steps to determine the individuals whose right to privacy had been violated by the bank, nor did it take any steps to notify individuals that their privacy had been violated and warn

them of steps to be taken to protect themselves against identity theft or other misuse of their sensitive personal information.

20. Employees of the bank continued to use the unsecured fax transmission lines and continued to send sensitive personal information by facsimile transmission to third parties after the complaint of the class member.

The Bank's Notification Through the Maryland Civil Suit

21. Throughout 2002, 2003 and into 2004, bank employees continued to use the unsecured facsimile transmission lines. Sensitive personal information of class members continued to be disclosed to third parties, without warning to, or consent of the class members. Allstar made further complaints to the bank. The bank took no steps to address its continuing breach of privacy of the class members.

22. In or about February of 2004, Allstar filed a civil suit against the bank in the State of Maryland, in the United States of America. This civil action sought damages against the bank for its continued sending of sensitive personal information of the class members by facsimile to Allstar.

23. Through the pleadings in the Maryland action and subsequent discovery, the bank again became aware of its violation of the right to privacy of many more of its clients. In spite of such knowledge, the bank took no steps to warn the class members of its breach of their right to privacy or of its disclosure, without consent, of sensitive personal information. The bank did not offer any advice to class members as to how they might protect themselves from identity theft or other misuse of their sensitive personal information.

24. The bank took no steps to protect the sensitive personal information which it knew to be in the possession of third parties from further unauthorized disclosure.

25. On or about November 8, 2004, the unauthorized facsimile transmission containing the plaintiff's sensitive personal information, along with that of another class member were electronically filed on a court web site in Maryland as part of an interlocutory motion. The information of the plaintiff and the other class member was available on the internet. Its further dissemination cannot be determined, however, in digital form, it could exist in multiple copies available throughout the internet and in caches on computers and servers linked to the internet.

26. The information made available on the internet included highly sensitive personal information of the plaintiff and another class member including their names, addresses, unpublished personal telephone numbers, their social insurance numbers, their RRSP-GIC numbers and amounts, their bank account numbers and a digital representation of their personal signatures.

27. Yet again, the bank took no steps to warn the plaintiff or the other class members of this further violation of their right to privacy.

28. On or about November 24, 2004, the plaintiff was contacted by a member of the press. The member of the press requested an interview of the plaintiff with respect to the sensitive personal information of the plaintiff which was now available on the internet. The member of the press advised that he intended to report on the bank's violation of plaintiff's privacy in a televised newscast that evening.

29. The bank became aware of the newscast. Solely as a result of the anticipated negative publicity surrounding the bank's violation of a client's privacy and its multiple breaches of *PIPEDA*, the bank notified the Office of the Privacy Commissioner.

30. The bank took no steps to advise or warn the class members of its breach of their privacy or the steps they could take to protect themselves from identity theft or improper use of their sensitive personal information until after the Office of the Privacy Commissioner subsequently advised that an investigation would be instituted against the bank.

Breach of Contract

31. It was an implied term of the contracts between the class members and the bank that:

- (a) the bank would treat the personal information of the class members as confidential;
- (b) the bank would handle the personal information of the class members in accordance with its published privacy policies;
- (c) the bank would treat the personal information of the class members in accordance with all legislation governing the collection and disclosure of personal information;
- (d) the bank would not disclose the class member's personal information without their consent.

32. The breach of privacy in sending sensitive personal information of the class members to third parties without the consent of the class members constitutes breach of the contracts between the bank and the plaintiff and the class members.

Breach of PIPEDA and the Right to Privacy

33. The bank collects, uses or discloses the personal information of clients in the course of its commercial activities as a bank. The bank is subject to *PIPEDA*.

34. Under *PIPEDA*, the class members have a right to privacy and security of their personal information. The bank is under a duty to protect its clients' right to privacy and their personal information.

35. The sensitive personal information of the class members was disclosed by the bank. The class members were neither informed of, nor did they consent to the disclosure.

36. The bank did not protect the sensitive personal information of the class members with security safeguards appropriate to the sensitivity of the information.

37. The breach of the class members' privacy by the bank constitutes a breach of *PIPEDA* for which damages may be awarded.

Breach of Duty of Care

38. The bank owed a duty of care to the class members to treat their sensitive personal information in confidence and to prevent its disclosure to unauthorized third parties. The bank is in breach of the duty of care owed to the class members. This breach of duty occurred through the negligence of the bank or its employees, for whom the bank is liable, particulars of which are as follows:

- (a) the bank had inadequate privacy policies and procedures in place for the protection of its clients;
- (b) the bank had failed to properly apply and enforce its privacy policies and procedures in place for the protection of its clients;
- (c) the bank failed to train its employees on its privacy policies;

- (d) the bank failed to appropriately supervise and oversee its employees in their implementation of the bank's privacy policies and procedures;
- (e) the bank permitted its employees to use unsecured facsimile telephone lines for the sending of sensitive personal information;
- (f) the bank failed to train its employees on proper use of unsecured facsimile machines;
- (g) the bank failed to implement appropriate technologies to protect the personal information of clients including the use of encryption and the use of dedicated, secure, communication lines for transfer of sensitive personal information;
- (h) employees of the bank negligently entered incorrect facsimile telephone numbers into the facsimile sending machines;
- (i) employees of the bank failed to follow up to determine if the facsimile transmissions were received at the intended destination;

- (j) the bank's central operations service group failed to follow up on facsimile transmissions which ought to have been received, but were not;
- (k) the bank failed to properly investigate the misdirected facsimile transmissions when the bank was advised such were occurring and continuing to occur;
- (l) the bank failed to warn the class members that their sensitive personal information had been disclosed to third parties without authorization;
- (m) the bank failed to advise class members of steps that they should take to minimize the risk of identity theft or improper use of sensitive personal information;
- (n) the bank failed to take steps to determine the extent to which it had violated the privacy of its clients and to identify those clients whose privacy had been violated; and
- (o) the bank failed to implement appropriate reporting structures and governance processes within the bank to ensure that senior management

was informed when the bank breached a client's right to privacy or when it breached *PIPEDA*.

Damages

39. The plaintiff and class members claim that the bank is liable and responsible for damages sustained through its breach of privacy of each class member.

40. The sensitive personal information of the class members has been disclosed and disseminated to unauthorized third parties. The class members have no means of determining how widely their information has been disseminated. Of particular concern is the dissemination, in digital form, of each class member's signature. Class members will be required to incur ongoing costs in monitoring their credit rating, bank accounts, RRSP accounts, in obtaining biannual reports from relevant credit rating agencies and in notifying financial institutions of the potential for identity theft. This monitoring will take time and the class members will incur costs. The class members claim for these ongoing costs and damages.

41. The class members entrusted the bank with their sensitive personal information in order to be secure and to obtain the peace of mind that their financial affairs were

protected by a well respected Canadian bank. The financial information at issue dealt particularly with Registered Retirement Savings Plans and other guaranteed investments on which the class members rely for their support and sustenance in their retirement years. Rather than bringing them the peace of mind that their financial affairs were protected by a well respected Canadian bank, the class members now find that their sensitive personal information has been needlessly disclosed. They were not told of the serious breach of their privacy. They are worried and concerned over identity theft and misuse of their personal information. The bank's breaches have caused significant emotional anxiety and distress to the class members. The class members claim damages for their emotional distress.

42. Further, and in the alternative, the plaintiff and the class members claim damages for humiliation arising out of the disclosure of their sensitive personal information. The plaintiff and the class members plead and rely on *PIPEDA* s.16.

43. Due to the egregious, high handed and contumelious conduct of the bank, including:

- (a) the bank's repeated refusal to properly secure the sensitive personal information of the class members;

- (b) the bank's failure to properly investigate after repeated warnings;
- (c) the bank's continuing violation of the right to privacy of the class members;
- (d) the bank's intentional failure to report its breaches of *PIPEDA* until its acts were about to be exposed by the media; and,
- (e) the bank's intentional failure to advise class members of its breach of their right to privacy until after it had been told that an investigation was going to be commenced by the Canadian Privacy Commissioner;

the plaintiff and the class members are entitled to recover punitive, aggravated and exemplary damages.

Statutes

44. The plaintiffs plead and rely upon the *Class Proceedings Act*, 1992, S.O. 1992, c. 6 and the *Personal Information Protection and Electronic Documents Act* (2000), c. 5.

45. The plaintiff proposes that the trial of this action take place in the City of Toronto, in the Province of Ontario.

DATE: February 4, 2005

MICHAEL E. GIRARD
Barrister & Solicitor
6 Adelaide Street East
Suite 710
Toronto, Ontario
M5C 1H6

Law Society No. 24643I
(416) 203-3127 (phone)
(416) 913-1886 (fax)

Solicitor for the plaintiff

THEODORE JOEL SPEEVAK

- and -

CANADIAN IMPERIAL BANK OF COMMERCE

Plaintiff

Defendant

Court File No.

05-CV-28348JCP

ONTARIO
SUPERIOR COURT OF JUSTICE

Proceedings commenced at Toronto

STATEMENT OF CLAIM

Proceeding under the *Class Proceeding Act*, 1992

MICHAEL E. GIRARD
Barrister & Solicitor
6 Adelaide Street East
Suite 710
Toronto, Ontario
M5C 1H6

Law Society No. 246431
(416) 203-3127 (phone)
(416) 913-1886 (fax)

Solicitor for the plaintiff