No. *Court File No.* ***VLC-S-S-238293***

Vancouver Registry

IN THE SUPREME COURT OF BRITISH COLUMBIA

BETWEEN

MARTIN L'ANTON

Plaintiff

AND

MACKENZIE FINANCIAL CORPORATION and INVESTORCOM INC

Defendant(s)

Brought under the *Class Action Proceedings Act,* [R.S.B.C. 1996], c. 50

NOTICE OF CIVIL CLAIM

This action has been started by the plaintiff(s) for the relief set out in Part 2 below.

If you intend to respond to this action, you or your lawyer must

(a) file a response to civil claim in Form 2 in the above-named registry of this court within the time for response to civil claim described below, and

(b) serve a copy of the filed response to civil claim on the plaintiff.

If you intend to make a counterclaim, you or your lawyer must

(a) file a response to civil claim in Form 2 and a counterclaim in Form 3 in the above-named registry of this court within the time for response to civil claim described below, and

(b) serve a copy of the filed response to civil claim and counterclaim on the plaintiff and on any new parties named in the counterclaim.

JUDGMENT MAY BE PRONOUNCED AGAINST YOU IF YOU FAIL to file the response to civil claim within the time for response to civil claim described below.

Time for response to civil claim

A response to civil claim must be filed and served on the plaintiff(s),

a) if you were served with the notice of civil claim anywhere in Canada, within 21 days after that service,

b) if you were served with the notice of civil claim anywhere in the United States of America, within 35 days after that service,

c) if you were served with the notice of civil claim anywhere else, within 49 days after that service, or

d) if the time for response to civil claim has been set by order of the court, within that time.

CLAIM OF THE PLAINTIFF

Part 1: STATEMENT OF FACTS

Parties and Overview

1. This action arises out of a cyber security breach (the "**Breach**") that occurred in or about February 2023. A cybercriminal group exfiltrated the personal information of former and current customers of MacKenzie Financial Corporation "**MacKenzie**") located on the servers of InvestorCOM. The data was supplied to InvestorCOM by MacKenzie and then stored in the databases of its GoAnywhere software.

2. GoAnywhere is a file transfer system/platform offered as a secure managed file transfer (MFT) product by its owner Fortra LLC that "streamlines the exchange of data between systems, employees, customers and trading partners" according to the company. The software is intended to help organizations of all sizes streamline and secure their data transmissions with automated file transfer software.

3. InvestorCOM Inc. is a company which licenses the use of GoAnywhere and provides data transfer services relating to wealth and asset management to investment companies, including in its capacity as a vendor to MacKenzie.

4. The cybercriminals accessed and stole information from the servers of InvestorCOM Inc. about customers of MacKenzie including the social insurance numbers (SIN) of thousands of customers, along with their MacKenzie account numbers, names, and addresses (the "S**tolen Information**").

The Plaintiff

5. The plaintiff, Martin L'Anton, is a resident of Vancouver, British Columbia. He purchased MacKenzie mutual funds through his investment advisor.

6. On or about May 4, 2023, he received a letter from MacKenzie stating that his personal information, including his social insurance number had been stolen by hackers as part of a cyber security incident. MacKenzie collected his personal information because his investment advisor, acting as Mr. L'Anton's agent, completed an application where his personal information was provided to MacKenzie.

7. The letter recommended that he sign up for Trans Union credit monitoring and offered a code to do so. He signed up for Trans Union, although doing so was difficult and time consuming due to the demand for the service after the hack.

8. He also signed up for Equifax, at an ongoing cost of $25/month, as Trans Union does not cover off all credit-granting institutions. This was a difficult and time-consuming process for Mr. L'Anton who was eventually required to call Equifax directly in order to resolve technical issues that initially prevented him from signing up.

9. Mr. L'Anton used a private wealth manager for his investments. He expected that MacKenzie, one of the funds he chose to invest with, would work to maintain his privacy and protect the security of his information.

The Defendants

InvestorCOM

10. The defendant InvestorCOM Inc. ("InvestorCOM"), is a company that provides regulatory compliance software and communications solutions for financial services, such as wealth and asset management. InvestorCOM has offices in Toronto, Ontario and lists its headquarters in Brantford, Ontario.

11. Their technology was developed in response to increasing regulation and the demand for more effective communication and disclosure from the financial service industry.

12. Investment companies all over the world, including Canada, use their technology for wealth and asset management. In this particular instance, InvestorCOM contracted with Fortra to use Fortra's GoAnywhere software. InvestorCOM used the GoAnywhere software to provide data transfer services to its clients, including its Canadian clients.

MacKenzie

13. The defendant MacKenzie is a leading investment management firm providing investment advisory and related services to retail and institutional clients. It was founded in 1967 and has offices across Canada including Vancouver, British Columbia, USA, Dublin, London, Hong Kong, and Beijing. Its Canadian headquarters is located at 180 Queen Street West, Toronto, Ontario. MacKenzie distributes its investment services through multiple distribution channels to both retail and institutional investors.

14. The company manages and administers more than 100 investment funds, including mutual funds, segregated funds, pooled funds, pension funds, labour sponsored funds and structured products as well as an array of loan and deposit services. MacKenzie's core business is managing mutual funds on behalf of investors throughout North America.

15. MacKenzie was a client of InvestorCOM who is a service provider for MacKenzie.

CLASS DEFINITION

16. The proposed class action is brought on behalf of <u>current or former Canadian customers of MacKenzie</u> who were notified by MacKenzie their information may have been compromised in the Breach. The proposed class is defined as any individual resident in Canada who received notice from MacKenzie that their information may have been compromised in the Breach.

FACTS

17. “GoAnywhere” is a managed file transfer system owned by Fortra LLC, a US-based company. GoAnywhere was used by InvestorCOM Inc. ("InvestorCOM"), a printing and delivery service provider for financial institutions, which provided services to MacKenzie.

18. On or about January 30, 2023, Fortra LLC discovered the Hacker had created unauthorized user accounts with customers of its managed file transfer service, GoAnywhere.

19. The unauthorized accounts allowed the hacker to access names, addresses and SIN numbers of individuals which had been shared using GoAnywhere and to download those files. These included records of individuals who had not held funds offered by MacKenzie for many years.

20. Fortra took impacted systems offline on January 31, 2023, stopping the unauthorized party’s ability to access the system.

21. Fortra notified InvestorCOM of the Breach and InvestorCOM, in turn, notified MacKenzie.

22. MacKenzie informed clients in a letter dated April 27, 2023, that a third-party vendor, InvestorCOM, was compromised by a cyber security incident related to data transfer supplier GoAnywhere.

23. After the data breach, MacKenzie offered two years of free identity and credit protection through TransUnion, a consumer credit reporting agency. Customers had until August 31, 2023, to sign up.

24. However, class members had problems accessing promised supports, as Trans Union sites struggled under the demand. Many spent up to 10 hours trying to sign up or found that their codes did not work (or were already used by other parties). In any event, not all Canadian banks use TransUnion. Credit protection does not prevent identity theft. It is intended to provide notice of questionable financial transactions.

25. In MacKenzie’s case, SIN numbers were available to be compromised because MacKenzie, contrary to industry practice, was using them as unique identifiers for clients when it transferred class member personal information to Fortra.

The Breach

26. As a result of the cyber security breach the plaintiff and class members personal information has been intentionally accessed by cybercriminals on a computer/server without authorization, including social insurance numbers, names, addresses, account numbers and, in some cases, dealer account numbers.

27. Upon being notified of the Breach, class members have experienced fear and apprehension, anxiety, anger, risk, and confusion in relation to the unauthorized or unknown future use of their personal information. To mitigate the risk class members have taken all reasonable steps necessary to protect their credit reputation and secure their finances including hours of wasted time, lost income and inconvenience involved in applying for and the cost of credit monitoring and applying for a new social insurance number from Service Canada.

28. Given that the personal information was stolen by cybercriminals and relates to investors who held financial products there is a real and substantial risk or chance that class members have or will be the victims of fraudulent schemes resulting in identity theft or financial fraud, and class members will experience wasted time and inconvenience in responding to the theft, reporting it and arranging for new social insurance numbers.

29. SINs are necessary in Canada to access government programs. They are permanent and not easily canceled or changed, unlike, for example, credit cards, and therefore have long lasting value to malicious actors, which creates an increased risk to impacted individuals. They can be used to open fraudulent accounts, loans, credit cards, etc., even years later. In this case, the SINs were stolen in conjunction with other identifying information, thereby increasing the risk to impacted individuals.

The Contract

30. Class members contracted with MacKenzie directly or through investment agents to purchase or trade in certain types of investment vehicles. Through this process, class members provided personal information to MacKenzie in order to fulfill reporting and know-your-client requirements.

31. Class members or their agents completed an "application form" which included MacKenzie's Privacy Protection Notice ("**PPN**"), which formed part of the contract between the investor and MacKenzie. As part of the application, clients stated that "I acknowledge reading the Privacy Protection Notice on the reverse side of this application form and I consent to my personal information being collected, held, used and disclosed by MacKenzie in the ways and for the purposes identified in the Privacy Protection Notice."

32. The provision of this personal information was also governed by MacKenzie's parent company's privacy policy summary ("**PPS**"), which explicitly states that it applies to "clients" and is included in the contract by implication as it sets out how the personal information will be protected.

The PPN

33. In addition to being included in MacKenzie's investment applications, the PPN is publicly available on MacKenzie's website and linked to in the PPS. The PPN provides that "MacKenzie … is committed to protecting the privacy of personal information that we collect and maintain in the course of carrying on our business. This Notice describes how we collect, hold, use, and disclose your personal information."

34. The PPN provides that "MacKenzie may transfer your personal information for the purposes identified in this Notice to our service providers, such as account statement preparation and mailing companies, courier companies, imaging companies, and document storage companies. When MacKenzie transfers personal information to our service providers, we ensure by contractual means that the transferred personal information is used only for the purposes for which the service provider is retained and <u>is protected</u> to the same degree as it is when in our possession." (emphasis added).

35. It further provides that "MacKenzie may disclose your personal information for the purposes identified in this Notice to third parties such as your Dealer, third party service providers, data-processing firms, other companies in the MacKenzie Group of Companies, other financial institutions and mutual fund companies, and group plan administrators." The purposes are identified in Section 3 of the PPN and include:

A. identifying you and ensuring the accuracy of information contained in your client record;
B. establishing and administering your account, determining, maintaining, recording, and storing account holdings and transaction information in your client record;
C. executing transactions with or through MacKenzie including transferring funds by electronic or other means;
D. providing you and your Dealer with account statements, transaction confirmations, tax receipts, financial statements, proxy mailings, registered plan notices, and other information which you or your Dealer may request as needed to service your account;
E. verifying information previously given by you with any other organization when necessary for the purposes provided in this Notice;
F. processing pre-authorized debit transactions;
G. collecting a debt owed to MacKenzie;
H. engaging in the financing or sale of all or part of our businesses, reorganizing our businesses, and obtaining and submitting insurance claims; and
I. meeting legal and regulatory requirements.

36. Personal information is not defined in the PPN but is defined in the PPS to include "any information about an identifiable individual. It includes but is not limited to name, date of birth, address, telephone number, social insurance number, banking information, income, assets, occupation, and any other know-your-client information."

37. With respect to Social Insurance Numbers ("**SINs**"), the PPN provides that "By law, MacKenzie is required to use your SIN when submitting tax reports to the Canada Revenue Agency. We may use your SIN as an identifier for reasons such as consolidating your holdings so that fees associated with your account are reduced or are not charged more than once, or that your mailings are delivered in one envelope or are not duplicated. Also, we may share your SIN as a unique identifier for the purposes identified in this Notice to third parties such as your Dealer, group plan sponsor, and third party service providers."

The PPS

38. Although the PPN refers to MacKenzie's policies on retention and protection of personal information, these are not actually set out in the PPN. Instead, they are set out in the PPS, which, by implication, formed part of the contract between class members and MacKenzie. The PPS was prepared by MacKenzie's parent company, IGM Financial Inc., and sets out privacy policies for IGM's companies, including MacKenzie.

39. The PPS identifies its purpose as to "to provide information on how … MacKenzie Financial Corporation … operate[s] in compliance with applicable federal and provincial privacy legislation." The PPS sets out 10 principles (based on the principles of PIPEDA) by which MacKenzie will operate.

40. The PPS defines "client" to include "any individual about whom IGM Companies collect and maintains personal information, including but not limited to current, former and prospective clients."

41. Under the first principle, Accountability, the PPS states that its personnel "shall … seek consent from the Client (for collecting, using, and disclosing personal information) in such a way so that the Client can reasonably understand how the personal information will be used and disclosed…"

42. Under principle 5, "Limiting Use, Disclosure and Retention", the PPS states that "personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the Client or as required by the law. personal information shall be retained only as long as necessary for fulfillment of those purposes or as required by law." It goes on to state that "IGM Companies remain responsible for personal information while in the possession of third parties and protect the information through contracts to ensure comparable levels of protection provided by IGM."

43. Under principle 7, Safeguards, the PPS states that "personal information shall be protected by security safeguards appropriate to the sensitivity of the information. These safeguards shall protect against loss, theft, unauthorized access, use, disclosure, copying or modification of personal information, regardless of the format in which it is held." The PPS states that this will be accomplished through:

    a) Physical measures – restrict access to offices or areas where personal information may be accessible and lock filing cabinets.

    b) Organizational Measures – use of security clearances, limiting access to information on a need-to-know basis based on job roles, and evaluating periodically whether security clearance or access to applications with personal information is still required.

c) Technological Measures – use of passwords, encryption, firewalls and effective systems standards and oversight.

d) Contractual Measures – ensure contracts with third party service providers contain privacy provisions to protect personal information while in their custody and systems standards are met.

44. Finally, under principle 10, "Challenging Compliance", the PPS describes steps to be taken if there is a breach of its security safeguards. IGM companies, such as MacKenzie, are required to assess "whether a breach poses a real risk of significant harm." Significant harm is defined as "bodily harm; humiliation; damage to reputation and relationships; loss of employment, business or professional relationships; financial loss or loss of property; identify theft; or negative effects on credit records."

45. When MacKenzie assesses that there is a "real risk of significant harm," then it is required to "notify affected Clients in a timely manner when a privacy breach has occurred and is determined to pose a real risk of significant harm to the individual." It is also required to "notify the federal Privacy Commissioner and/or the provincial Privacy Commissioner(s), where applicable, if a breach of personal information is determined to pose a real risk of significant harm to impacted Clients."

46. In this case, in its letter to notify affected clients, MacKenzie warned clients and former clients that they should:

a) Remain vigilant to the risk of phishing…

b) Use strong passwords for personal and financial accounts.

c) Avoid using the same passwords.

d) Change your passwords regularly.

PART 2 – RELIEF SOUGHT

47. The plaintiff on his own behalf and on behalf of the class members, claim:

a) an order pursuant to the *Class Proceedings Act [RSBC 1996] Chapter 333* (the "*CPA*"), certifying this action as a class proceeding and appointing the plaintiff as representative plaintiff of the Class;

b) a declaration that the defendants owed a duty of care to the plaintiff and the class members, and breached the standard of care owed to them;

c) a declaration that the defendants breached their agreement/contracts with class members;

d) a declaration that MacKenzie breached the confidence of the class members;

e) a declaration that MacKenzie intruded upon the seclusion of the class members;

f) a declaration that MacKenzie breached the *Privacy Act*, R.S.B.C. 1996 c. 373; *The Privacy Act*, CCSM, c. P125, *The Privacy Act*, RSS 1978, c. P-24, and *The Privacy Act*, RSNL 1990, c. P-22;

g) general and special damages;

h) an order directing an aggregate assessment of damages;

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

j) pre-judgment and post-judgment interest;

k) the costs of administering the plan of distribution of the recovery in this action; and

l) such further and other relief as this Honourable Court deems just.

PART 3 – LEGAL BASIS - CAUSES OF ACTION

NEGLIGENCE

MacKenzie

48. class members contracted with MacKenzie directly or through investment agents to purchase or trade in certain types of investment vehicles. Through this process, class members provided personal information to MacKenzie.

49. MacKenzie then transferred the personal information to InvestorCOM through their use of the GoAnywhere File transfer system.

50. Pursuant to section 4.1.3 of PIPEDA, MacKenzie, a Canadian Corporation which collected data and transferred it to InvestorCOM remains responsible for protecting the personal information originally under their control. In these circumstances, the plaintiff pleads that MacKenzie is liable for the negligent acts of InvestorCOM as hereinafter described and owed a duty of care to the class members as hereinafter described.

51. MacKenzie owed a duty of care to the class members in their collection, use and retention of the personal information, to keep the personal information confidential and secure, and to ensure that when it was transferred to InvestorCOM it would not be lost, disseminated or disclosed to unauthorized persons and to delete and destroy personal information of customers who cancelled their investments.

52. Specifically, this defendant owed a duty of care to the class members to take reasonable steps to establish, maintain and enforce appropriate security safeguards against a cyberattack, to ensure that any entity which it entrusted with personal information did the same, and to take appropriate steps to limit the exposure of the class members' personal information even in case of a successful cyberattack.

53. There was a sufficient degree of proximity between the class members and MacKenzie to establish a duty of care because:

    a) it was reasonable for the plaintiff and other class members to expect that MacKenzie had implemented appropriate security safeguards against a

cyberattack and to limit the exposure of their personal information in case of a cyberattack, especially where the defendants held themselves out to class members as having rigorous privacy standards to protect applicants' and customers' privacy;

b) it was reasonably foreseeable to MacKenzie that, if a cyberattack resulted in the theft of the class members' personal information, the class members would sustain damages, such that the defendant should have been mindful of the class members' privacy and on guard against a cyberattack.

c) it was reasonably foreseeable to MacKenzie that, if it failed to take appropriate security measures and to implement programs and policies designed to protect personal information, or to ensure that parties that it contracted with did the same, there was a risk that the class members' privacy would be breached, because of the sensitivity of the types of data collected and stored, and the climate of increasing cyberattacks targeted toward institutions which collect sensitive and private information;

d) In particular, it was reasonably foreseeable to MacKenzie that if personal information was not removed and/or deleted from the GoAnywhere software after a transaction, it would remain in the software and be available to any party which obtained access to that software, such as the hacker;

e) the class members were entirely vulnerable to MacKenzie, in terms of relying on MacKenzie to take appropriate security measures to protect their personal information;

f) there was a contractual relationship between the class members and MacKenzie;

g) MacKenzie, through its respective agreements and/or contracts with class members, promised to take appropriate measures to protect the class members' personal information;

h) there is a sufficient degree of proximity between the class members and the defendants because the class members are, or were, customers of the defendants;

i) the defendants were required by sections 4.1, 4.5 and 4.7 of Schedule 1 to the *personal information Protection and Electronic Documents Act*, S.C. 2000, c. 5 (the "*PIPEDA*"), to implement safeguards appropriate to the sensitivity of the information stored on their network;

j) It was reasonable for customers to expect MacKenzie would destroy and delete personal information when the need to have class members personal information was over and would instruct companies it contracted with to do the same.

54. MacKenzie failed in its duty to implement an appropriate standard of care in establishing adequate security safeguards in collecting, managing, storing, securing and/or deleting the class members' personal information, particulars being described below:

a) it failed to handle the collection, retention, security and disclosure of the class members' personal information in accordance with their obligations under the contract and PIPEDA;

b) it failed to handle the collection, retention, security and disclosure of the class members' personal information in accordance with their promises to class members;

c) it allowed the personal information to be used and disclosed for purposes other than those for which it was collected, contrary to s. 4.5 of Schedule 1 to the *PIPEDA*;

d) it failed to keep the class members' personal information secure and confidential;

e) it allowed class members' personal information to be stored on a network with known vulnerabilities;

f) it failed to encrypt the class members' personal information;

g) it failed to protect the class members' personal information from compromise, disclosure, loss or theft;

h) it failed to have a vendor risk management policy in place ;

i) it failed to properly scrutinize InvestorCOM's risk assessment policies and penetration testing strategies;

j) it failed to confirm that InvestorCOM had sufficient basic security controls;

k) it used class member social insurance numbers as personal identifiers when it supplied personal information to InvestorCOM when it knew or ought to have known other means were available to identify customers without exposing customers to the risk of compromised SIN numbers.

l) it failed to take steps to prevent the class members' personal information from being lost, disseminated, or disclosed to the public and unauthorized persons, and from being posted on the internet;

m) it failed to delete and destroy the personal information of class members when there was no longer a proper purpose for retaining the personal information; and

n) breaches of contract as particularized below;

InvestorCOM

55. InvestorCOM contracted with MacKenzie to provide services to them using Fortra's GoAnywhere software. InvestorCOM received class member personal information for use with the GoAnywhere software.

56. InvesterCOM owed a duty of care to the class members in their collection, use and retention of the personal information, to keep the personal information confidential and secure, and to ensure that it would not be lost, disseminated or disclosed to unauthorized persons and to delete and destroy personal information of customers who cancelled their investments.

Specifically, this defendant owed a duty of care to the class members to take reasonable steps to establish, maintain and enforce appropriate security safeguards against a cyberattack, and to take appropriate steps to limit the exposure of the class members' personal information even in case of a successful cyberattack.

57. There was a sufficient degree of proximity between the class members and InvestorCOM to establish a duty of care because:

a) it was reasonable for the plaintiff and other class members to expect that any company who received their personal information from MacKenzie for storage and file transfer purposes including InvestorCOM had implemented appropriate security safeguards against a cyberattack and to limit the exposure of their personal information in case of a cyberattack, especially where the defendant MacKenzie held itself out to class members as having rigorous privacy standards to protect applicants' and customers' privacy and would ensure any third party with whom it shared personal information would maintain the same standard;

b) it was reasonably foreseeable to InvestorCOM that, if a cyberattack resulted in the theft of the class members' personal information, the class members would sustain damages, such that the defendant should have been mindful of the class members' privacy and on guard against a cyberattack.

c) it was reasonably foreseeable to InvestorCOM that, if it failed to take appropriate security measures and to implement programs and policies designed to protect personal information, there was a risk that the class members' privacy would be breached, because of the sensitivity of the types of data collected and stored, and the climate of increasing cyberattacks targeted toward institutions which collect sensitive and private information;

d) In particular, it was reasonably foreseeable to InvestorCOM that if personal information was not removed and/or deleted from the GoAnywhere software after a transaction, it would remain in the software and be available to any party which obtained access to that software, such as the hacker;

e) the class members were entirely vulnerable to InvestorCOM, in terms of relying on them to take appropriate security measures to protect their personal information;

f) InvestorCOM, through its agreements and/or contracts with MacKenzie, promised to take appropriate measures to protect the class members' personal information;

g) there is a sufficient degree of proximity between the class members and InvestorCOM because InvestorCOM is in the business of dealing directly with the personal information of individuals;

h) It was reasonable for customers to expect InvestorCOM would destroy and delete personal information when the need to have class members personal information was over.

58. InvestorCOM failed in its duty to implement an appropriate standard of care in establishing adequate security safeguards in collecting, managing, storing, securing and/or deleting the class members' personal information, particulars being described below:

a) it failed to handle the collection, retention, security and disclosure of the class members' personal information in accordance with industry standards;

b) it used class members' SINs as personal identifiers, contrary to its obligation to protect class members' data;

c) it retained class members' personal information longer than necessary for the purposes for which it was collected;

d) it failed to implement appropriate physical, organizational and technological safeguards to protect the personal information against loss, theft, unauthorized access, disclosure, copying, use, and/or modification, as particularized in contrary to s. 4.7 of Schedule 1 to the *PIPEDA*;

e) it failed to use any, or appropriate, cybersecurity measures, programs and policies to safeguard the class members' personal information, or it used

cybersecurity measures, programs and policies which were outdated, inadequate, and below the reasonable industry standards;

f) it failed to hire competent employees, it failed to properly supervise their employees, or it failed to provide proper training to its employees

g) it allowed the personal information to be used and disclosed for purposes other than those for which it was collected, contrary to s. 4.5 of Schedule 1 to the *PIPEDA*;

h) it failed to keep the class members' personal information secure and confidential and it failed to fulfill its contractual obligations to MacKenzie to keep class members' personal information secure and confidential;

i) it allowed class members' personal information to be stored on a network with known vulnerabilities;

j) it failed to encrypt the class members' personal information;

k) it failed to protect the class members' personal information from compromise, disclosure, loss or theft;

l) it failed to take steps to prevent the class members' personal information from being lost, disseminated, or disclosed to the public and unauthorized persons, and from being posted on the internet; and

m) it failed to delete and destroy the personal information of class members when there was no longer a proper purpose for retaining the personal information;

Causation and Damages

As a direct result of the defendants joint and several negligence the class members personal information was stolen by cybercriminals causing the class to sustain damages. The plaintiff pleads the defendants are joint tortfeasors under the Negligence Act of BC and equivalent provincial legislation.

BREACH OF CONTRACT

MacKenzie

59. Throughout the class period the plaintiff and every class member who had an account with MacKenzie entered into a standard form contract with MacKenzie either directly or through an agent by filling out an application which included the PPN and, by implication, the PPS. In each case, the contract was a "take it or leave it" contract of adhesion, drafted by MacKenzie and, as plead above, provided either to the client directly or to the client's agent.

60. The relevant provisions of the contract, including the PPN and PPS, are set out above at paragraphs 31 to 45.

61. MacKenzie's contracts with class members had the following express or implied terms:

    a) That MacKenzie would comply with its own privacy policies and with applicable privacy laws;

    b) That MacKenzie would provide strict safeguards and rigorous privacy and security standards to protect personal information and prevent identity theft and unauthorized access;

    c) That MacKenzie would encrypt user data to prevent identity theft and unauthorized access to personal information;

    d) That MacKenzie would not retain personal information longer than needed;

    e) That MacKenzie would hold third-party contractors (such as InvestorCOM) to the same standards;

    f) That MacKenzie would comply with PIPEDA; and

    g) That MacKenzie incorporated PIPEDA into its contracts by reference in the PPN and PPS. The references in the PPS and PPN make it clear that they were incorporating the principles of PIPEDA into the contract.

62. MacKenzie breached the express or implied terms of its contracts by:

a) It failed to encrypt user data, and permitted InvestorCOM to retain the personal information with insufficiently strict safeguards and privacy and security standards;

b) It failed to delete user data after it was no longer needed and did not ensure that InvestorCOM did so when provided with personal information;

c) It provided client SINs to third party vendors without consent because there was no purpose listed under section three of the PPN in which class members authorized MacKenzie to share SINs;

d) In the alternative, it did not obtain meaningful consent within the meaning of principle 4.3 of PIPEDA to share SINs as identifiers with InvestorCOM;

e) It retained class members personal information longer than was necessary, and in particular, after their relationship with customers ended; and

f) Failed to hold InvestorCOM to the same requirements.

63. Had MacKenzie fulfilled its contractual obligation to comply with PIPEDA the information would not have been available to be infiltrated, hacked, or extracted.

InvestorCOM

64. MacKenzie and InvestorCOM entered into a contract whereby InvestorCOM agreed to protect the personal information “to the same degree” as when it was in MacKenzie’s possession, including any safeguards described in the PPN and PPS.

65. InvestorCOM was familiar with the PPS and PPN when it entered into its contract with MacKenzie.

66. Class members were the intended beneficiaries of this contract between MacKenzie and InvestorCOM. This intention is evidenced by the explicit references in the PPN to MacKenzie contracting with third parties to protect “your personal information” and in the PPS to the fact that MacKenzie remains “responsible for personal information while in the possession

of third parties and protect the information through contracts to ensure comparable levels of protection provided by [MacKenzie]."

67. As a result, class members are third party beneficiaries of the contract between MacKenzie and InvestorCOM and may rely on the contract and sue in relation to its breach.

68. InvestorCOM's contract with the class was made on the same terms and breached in the same ways as set out above for MacKenzie.

BREACH OF CONFIDENCE

MacKenzie

69. Class members were invited to provide personal information to MacKenzie including name, address, postal code, phone number, email address, date of birth, occupation, and Social Insurance Numbers, which was then provided by MacKenzie to InvestorCOM. This information was provided to MacKenzie solely for the purpose of complying with regulatory requirements in the purchase of the various investment products offered by MacKenzie.

70. The class members' information was imparted to MacKenzie in circumstances in which an obligation of confidence arose, and in which the plaintiff and the class members could have reasonably expected their confidential information would be held in confidence. Class members were assured in their contracts that MacKenzie would keep their information confidential and secure.

71. Class members' information was confidential, exhibited the necessary quality of confidence, was not public knowledge, and involved sensitive private details about the personal affairs of the class members.

72. Class members' information was imparted to MacKenzie in circumstances in which an obligation of confidence and trust arose between investment advisor and client constituting a fiduciary relationship and an explicit assurance MacKenzie would keep the information confidential.

73. MacKenzie' assurances to class members were contained in the PPS and PPN, both of which reference PIPEDA and its obligations to class members and the scope of its permissions to

use class members' information were bounded by the requirements in sections 4.5, 4.7 and 5 of Schedule 1 of PIPEDA, as outlined above. This is because MacKenzie incorporated PIPEDA into its contracts with class members. In the alternative, if MacKenzie is found not to have incorporated PIPEDA in its contracts, the plaintiff pleads that the requirements of PIPEDA are mandatory on MacKenzie pursuant to division 1, subsection 5(1) of *PIPEDA*, S.C. 2000, c. 5.

74. MacKenzie knowingly and intentionally used class members confidential information, in particular class members' SINs, for a non-permitted use. It did so in a number of ways:

    a) by providing InvestorCOM with SINs absent consent and contrary to PIPEDA sections 4.5, 4.7 and 5 of Schedule 1 of PIPEDA;

    b) by allowing and/or directing InvestorCOM to use SINs as personal identifiers; and

    c) by allowing InvestorCOM to retain the Stolen Information, including SINs, long after class members had cancelled their accounts and/or after there was a need to retain it, contrary to section 5 of PIPEDA.

75. Therefore, MacKenzie misused confidential personal information to the detriment of the class who suffered a breach of their informational privacy because a cybercriminal group gained unauthorized access to confidential personal information as a result of MacKenzie using the information for an improper purpose.

76. Class members suffered additional detriment comprised of worry, distress and anxiety over the disclosure of confidential information to cyber criminals, financial harm,out of pocket expense and the real and substantial risk of financial harm and /or pecuniary damages incurred as a result being the victim of a crime.

77. MacKenzie is therefore liable for the tort of breach of confidence.

INTRUSION UPON SECLUSION AGAINST THE HACKER

78. The tort of intrusion upon seclusion is made out because:

    a) the Hacker intentionally invaded the class members' privacy;

b) the class members' personal information was invaded without lawful justification for invading the class members' private affairs or concerns; and

c) the personal information that was invaded is highly sensitive and personal and a reasonable person would consider the invasion to be highly offensive causing anguish, humiliation or distress.

Sensitivity of the personal information/The matters intruded upon were Private

79. The exfiltrated information included two categories of information, personal information, and social insurance numbers. The combined effect of the categories results in identifiable information taking on increased sensitivity when it is combined with SIN's.

80. Both categories of information take on an even higher degree of sensitivity especially because social insurance numbers can be used to steal a persons' identity and other types of fraud, apply for a credit card, open a bank account, receive government benefits such as CPP, employment insurance, to receive tax refunds, to work illegally or to obtain credit, and ruin credit ratings.

The Intrusion was Highly Offensive to a Reasonable Person

81. The degree of the intrusion was significant because the data was stolen by cybercriminals. The extracted data put each Class Member at risk of identity theft and becoming the subject of phishing attacks and scams. class members experienced distress, humiliation, anguish, reduced trust, feelings of lost privacy, and ongoing increased levels of stress.

82. The context of the unauthorized access to the information is a setting where, based on the defendants' privacy policies and its status as one of the largest investment companies in Canada, people had a reasonable expectation of high levels of privacy protection and confidentiality.

83. The conduct and circumstances of the invasion were the defendants' lax cyber security practices. The objective of the cyber-attack was to steal class member information.

84. The objectives and expectations of the class members whose privacy was invaded was guided by the defendants' assurances the personal information was safe and the class could place their trust in MacKenzie and its vendors.

STATUTORY ACTIONS FOR BREACH OF PRIVACY AGAINST THE HACKER

85. The plaintiff relies on the following statutory claims on behalf of the class members who are domiciled in, or are residents of the Provinces of British Columbia, Manitoba, Saskatchewan, and Newfoundland and Labrador.

British Columbia class members

86. The plaintiffs plead on behalf of all class members who are domiciled or are residents of the Province of British Columbia, that the Hacker violated section 1 of the *Privacy Act*, RSBC 1996, c. 373, as amended when it substantially, unreasonably, and without a claim of right accessed class members' personal information without class members' consent.

Manitoba class members

87. The plaintiffs plead on behalf of all class members who are domiciled or are residents of the Province of Manitoba that the Hacker violated sections 2 of the *Privacy Act*, CCSM c. P125, as amended when it substantially, unreasonably, and without a claim of right accessed class members' personal information without class members' consent.

88. As a result of this breach the Manitoba class members are entitled to rely upon section 4 of the *Privacy Act*, CCSM c. P125, as amended.

Saskatchewan class members

89. The plaintiffs plead on behalf of all class members who are domiciled or are residents of the Province of Saskatchewan, that the Hacker violated section 2 of the *Privacy Act*, RSS 1978, c. P-24, as amended 1996 when it without a claim of right willfully violated the privacy of the Saskatchewan class members by accessing class members' personal information without class members' consent.

Newfoundland and Labrador class members

90. The plaintiffs plead on behalf of all class members who are domiciled or are residents of the Province of Newfoundland and Labrador, that the Hacker violated section 3 of the *Privacy Act*, RSNL 1990, c. P-22, as amended when it, without a claim of right, accessed class members' personal information without class members' consent, and contrary to its duties to class members under the relevant contracts.

Negligence Acts – Against All Defendants and The Hacker

91. As a direct result of the defendants' negligent data base security practices the Hacker was able to invade/gain access to the class members' personal information, resulting in the class members sustaining damages for the torts of intrusion upon seclusion and breaches of privacy under the provincial privacy acts. But for the defendants' negligence the Hacker would not have invaded/gained access to the personal information.

92. Therefore, the tort committed by the defendants in negligence, combined with the tort(s) committed by the Hacker of intrusion upon seclusion and statutory breach of privacy, caused the class members to sustain damages rendering the defendants and the Hacker joint tortfeasors within the meaning of the Applicable Negligence Legislation.

93. The class members sustained indivisible injuries including moral damages and damages for breaches of the statutory causes of action under the privacy acts , out of pocket expenses, financial loss, damage to credit reputation, breach of informational privacy , damages to person or property, distress, humiliation, anguish, reduced trust, feelings of lost privacy, and ongoing increased levels of stress as a result of the combined tortious conduct of the tortfeasors rendering the defendants jointly and severally liable with the Hacker for the intrusion damages and breach of privacy damages sustained by the class members. These injuries have caused harm to the health, welfare, social, business, and financial positions of the class members.

94. The plaintiff pleads and relies on the *Negligence Act* [RSBC 1996] Chapter 333 section 4(2)(a); the *Negligence Act*, RSO 1990, c N.1, section 1; the *Contributory Negligence Act*, RSS 1978 c C-31, section 3(2); the *Contributory Negligence Act*, RSA 2000, c C-27, sections 1 and 2; the *Contributory Negligence Act*, RSNB 2011, c 131, sections 1 and 3; the *Tortfeasors and Contributory Negligence Act*, CCSM c T90, sections 2 and 5; the *Contributory Negligence Act*,

RSNS 1989, c 95, section 3; the *Contributory Negligence Act*, RSPEI 1988, c C-21, section 1; the *Contributory Negligence Act*, RSY 2022 c 42, section 1; the *Contributory Negligence Act*, RSNWT 1988, c C-18, sections 2 and 3; and the *Contributory Negligence Act*, RSNL 1990, c C-33, section 3 (collectively, the "**Applicable Negligence Legislation**")

BREACH OF THE *QUÉBEC CIVIL CODE ("CCQ")*

95. With regard to the class members resident in Québec, the defendants breached arts. 35, 36 and/or 37 of the *CCQ* by failing to obtain the consent of those class members to disclose their account and personal information.

96. The defendants breached arts. 35, 36, and 37 of the *CCQ* by failing to maintain adequate cybersecurity to safeguard the class members' account and personal information from unauthorized access.

97. More particularly, the defendants breached arts. 35, 36, and 37 of the *CCQ* because:

    a) it allowed unauthorized access to the account and personal information of the class members resident in Québec without their consent and without the invasion being authorized by law;

    b) it allowed unauthorized access to the correspondence, manuscripts, and other personal documents of class members resident in Québec; and

    c) it communicated the account Information of class members resident in Québec to unauthorized persons.

98. As a result of the breaches of the *CCQ*, the class members resident in Québec are entitled to moral and material damages pursuant to arts. 1457, and 1463-1464 of the *CCQ*.

99. Class members resident in Québec are also entitled to damages for breach of contract pursuant to art. 1458 of the *CCQ* for the reasons outlined above at paragraphs 59 to 68.

100. In addition, class members resident in Québec are entitled to punitive damages pursuant to article 49 of the *Charter of Human Rights and Freedoms*.

DAMAGES

101. As a result of the defendants' wrongdoing, the class members suffered damages including, but not limited to:

a) damages to credit reputation;

b) mental distress that is serious and prolonged;

c) fear, apprehension, anxiety, risk, anger, anguish and humiliation in relation to the unauthorized or unknown future use of their personal information;

d) costs incurred in preventing or rectifying identity theft or fraud;

e) out-of-pocket expenses;

f) wasted time, inconvenience, frustration and anxiety associated with taking precautionary steps to reduce the likelihood of identity theft, fraud or improper use of credit information;

g) time lost from employment engaging in precautionary communications with third parties such as credit card companies, credit agencies, banked and other parties and to inform said third parties of the potential that the class members' personal information may be misappropriated and to resolve any delays thereby caused;

h) nominal damages for breach of contract; and

i) Costs of purchasing credit monitoring and identity theft insurance.

102. In addition, the class members have suffered or will likely suffer further damages from identity theft and/or fraud because the personal information was stolen by cybercriminals for criminal purposes. It is likely or alternatively there is a real and substantial chance that these cybercriminals will use the personal information in the future for criminal purposes including identity theft. The type of information accessed and stolen in this attack can be used for fraudulent and other harmful purposes. SINs, which are permanent and not easily canceled, can be used to open fraudulent bank accounts, loans, credit cards, etc. Furthermore, the information taken in this cyber-attack included several different pieces of

information (e.g., banking information) that can be paired with other identifying information, thereby increasing the risk to impacted individuals. Addresses, phone numbers and emails can be used for additional phishing purposes, increasing an individual's vulnerability to identity theft and fraud.

103. The likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of a Hacker (deliberate intrusion). The Hacker in this matter is known to threaten exposure of stolen data by publishing it to websites that expose this information to additional malicious actors. Lack of evidence of misuse of the data does not mitigate against future harm. The harm in this matter is foreseeable as information obtained from a privacy breach can be published or used months or years after an incident.

104. It is likely or, alternatively, there is a real and substantial chance that in the future the personal information may be released or sold on the internet or used for criminal purposes such as to create fictitious bank accounts, obtain loans, secure credit cards or to engage in other forms of identity theft and/or fraud, thereby causing the class members to suffer damages.

Intrusion Upon Seclusion/Breach of the Privacy Acts / Breach of Confidence Damages

105. The plaintiffs claim damages for suffering, distress, humiliation, anguish, reduced trust, feelings of lost privacy, and ongoing increased levels of stress that it experienced from the unlawful intrusion, violations of the Privacy Acts and non -permitted use of their personal information caused by the defendants' wrongful acts. Pursuant to the applicable negligence acts, the plaintiffs are entitled to recover these damages from the defendants.

Disgorgement/Breach of Contract as Against MacKenzie

106. Class members have a legitimate contract interest in the defendant complying with its contractual obligations to protect unauthorized access, to keep private and confidential class members' personal information and to delete and destroy former customer information.

107. The nature of the class members contract interest is such that it cannot be vindicated by other forms of contractual relief and cannot possibly be quantified in monetary terms such

that the class members' interest in performance of the contract is not reflected by a pure economic measure.

108. In all the circumstances, other remedies would not adequately protect or vindicate the class members contractual right to control the dissemination of their own personal information, including:

a) Conventional contract damages alone would fail to deter the wrongdoer who through the drafting of the contracts has been prepared to misrepresent to class members how it would protect the privacy of their personal information and its retention policies and thereby gain by allowing class members' personal information to go at risk.

b) The class members relationship with the defendants engages trust, confidence, and vulnerability.

c) The class members have a legitimate interest in preventing the Defendant's profit-making activity.

d) The Defendant expressly contracted not to do the particular thing that permitted the breach; the purpose of the contract provision was breached; class members' rights were quasi-proprietary; and the personal information which should have been deleted and destroyed belonged to the class members but was used and retained unlawfully for the defendant's gain.

90. Therefore, the class members seek disgorgement of profits or revenues generated from the unlawful use of the class members' personal information.

91. It would be unconscionable for the defendants to retain the revenues generated by the conduct set out herein. Furthermore, the plaintiffs and class members have a legitimate interest in preventing defendants' profit-making activities, particularly where such activities relate to and incentivize defendants' breach of the class members' confidence and privacy rights, and any other wrongdoing as set out herein.

Nominal Damages for Breach of Contract

92. With respect to the claims for breach of contract, the plaintiff and the other class members seek nominal damages for breach of contract.

93. Nominal damages are appropriate here to affirm that there has been an infraction of class members' legal rights under the contracts. The plaintiff pleads that in the event there is no direct compensable loss to himself or to class members, an award of nominal damages for breach of contract is appropriate to vindicate rights.

STATUTES

94. The plaintiff pleads and relies upon the *CPA*, *PIPEDA*, the Applicable Negligence Legislation, the Provincial Privacy Acts and the *CCQ*.

THE PLACE OF TRIAL

95. The plaintiff proposes that this action be tried at the City of Vancouver.

Form 11 (Rule 4-5 (2))

ENDORSEMENT ON ORIGINATING PLEADING OR PETITION FOR SERVICE OUTSIDE BRITISH COLUMBIA

The plaintiff claims the right to serve this pleading/petition on the Defendants outside British Columbia on the ground that:

The circumstances in section 10 of the Court Jurisdiction and Proceedings Transfer Act are sections 10(e) because it concerns contractual obligations to a substantial extent were to be performed in British Columbia and by its express terms, the contract is governed by the laws of British Columbia; and 10 (h) concerns a business carried on in British Columbia

Plaintiff's address for service:	**CHARNEY LAWYERS PROFESSIONAL CORP.** 602 - 151 Bloor Street West Toronto, ON M5S 1S4
Fax number address for service (if any):	1-416-964-7416
E-mail address for service (if any):	tedc@charneylawyers.com
Place of trial:	Vancouver
The address of the registry is:	800 Smithe Street, Vancouver

Date: December 8, 2023

Ted Charney

Signature of Theodore P. Charney
lawyer for plaintiff

Rule 7-1 (1) of the Supreme Court Civil Rules states:

> (1) Unless all parties of record consent or the court otherwise orders, each party of record to an action must, within 35 days after the end of the pleading period,
>
> (a) prepare a list of documents in Form 22 that lists
>
> (i) all documents that are or have been in the party's possession or control and that could, if available, be used by any party at trial to prove or disprove a material fact, and
>
> (ii) all other documents to which the party intends to refer at trial, and
>
> (b) serve the list on all parties of record.

Appendix

[*The following information is provided for data collection purposes only and is of no legal effect.*]

Part 1: CONCISE SUMMARY OF NATURE OF CLAIM:

Proposed class action regarding damages suffered as a result of a cyber security breach which occurred in early 2023 wherein a hacker exfiltrated from the defendants the personal information of clients of the defendant, MacKenzie Financial Corporation.

Part 2: THIS CLAIM ARISES FROM THE FOLLOWING:

[*Check one box below for the case type that best describes this case.*]

A personal injury arising out of:

a motor vehicle accident

medical malpractice

X another cause

A dispute concerning:

contaminated sites

construction defects

real property (real estate)

personal property

the provision of goods or services or other general commercial matters

investment losses

the lending of money

an employment relationship

a will or other issues concerning the probate of an estate

X a matter not listed here

Part 3: THIS CLAIM INVOLVES:

[*Check all boxes below that apply to this case*]

X a class action

maritime law

aboriginal law

constitutional law

conflict of laws

none of the above

do not know

Part 4:

[*If an enactment is being relied on, specify. Do not list more than 3 enactments.*]

a) *Class Proceedings Act*, R.S.B.C. 1996, c. 50
b) *PIPEDA*, S.C. 2000 c. 5