No.
Vancouver Registry

IN THE SUPREME COURT OF BRITISH COLUMBIA

Between

YOUNG JIN LEE

PLAINTIFF

and

SIMON FRASER UNIVERSITY

DEFENDANT

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

NOTICE OF CIVIL CLAIM

(data breach)

This action has been started by the plaintiff 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 PRONOUCED 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,

(a) if you reside anywhere in Canada, within 21 days after the date on which a copy of the filed notice of civil claim was served on you,

(b) if you reside in the United States of America, within 35 days after the date on which a copy of the filed notice of civil claim was served on you,

(c) if you reside elsewhere, within 49 days after the date on which a copy of the filed notice of civil claim was served on you, or

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

THE PLAINTIFF'S CLAIM

Part 1: STATEMENT OF FACTS

Overview

1. Simon Fraser University ("**SFU**") is a comprehensive teaching and research university founded in 1965 with campuses located in Burnaby, Vancouver and Surrey, British Columbia. SFU has a student body of approximately 30,000 students, 6,500 faculty and staff and more than 160,000 alumni across Canada and around the world. On February 16, 2021, SFU advised their students, faculty, staff and alumni that, on February 5, 2021, an unauthorized party had gained access to personally identifiable information about Class Members' academic performance, financial aid details and other sensitive information (the "**Personal Information**"), in breach of Class Members' privacy and reasonable expectations (the "**Data Breach**"). The Personal Information was stored in an unencrypted Microsoft Excel spreadsheet. The Data Breach was the second such breach of data stored by SFU in the past year. Through this suit, Canadian residents seek to hold the Defendant accountable for the Data Breach.

The Parties

2. The Plaintiff is a resident of British Columbia. At material times before the Data Breach, he was a student at Simon Fraser University.

3. The Defendant Simon Fraser University is a corporation continued pursuant to the *University Act*, RSBC 1996 c. 468 and Regulations, with an address at 8888 University Drive, Burnaby, BC.

4. The Plaintiff brings this claim on his own behalf and on behalf of all Canadian residents whose Personal Information was accessed as a result of the SFU Data Breach ("**Class Members**").

Notice to the Plaintiff and Class Members of SFU's Data Breach

5. On February 16, 2021, SFU sent email notices to the known email addresses of the Plaintiff and Class Members announcing that, for the second time in a 12-month period, SFU had been subject to a cyberattack whereby an unauthorized party had gained access to one if SFU's servers and had gained exposure to Personal Information. The email included the following:

> On February 5, 2021 SFU staff discovered that there had been a cyberattack on one of SFU's servers. SFU IT Services immediately isolated the server and began an investigation. The investigation found that there was personally identifiable information stored among the data on this server and we are working to notify all impacted individuals.
>
> The following personally identifiable information about you was exposed:
>
> - Academic Career
> - Academic Program
> - Action Date
> - Admit Term
> - Aid Year
> - Application Date
> - Application Status
> - Award Amount
> - Campus
> - Computing ID
> - Current Indicator
> - Date Received

- Degree
- Degree Type
- Description
- Effective Date
- Employee/Student Number
- Faculty
- First Name
- Identification Method
- Internal External Indicator
- Internal Transfer
- Last Name
- Preferred First Name
- Previous Academic Program
- Previous Faculty
- Primary Program
- Program Action
- Program Action Reason
- Program Status
- Requestor
- Requirements Term
- Term
- Transcript Level
- Transcript Type
- Undeclared Indicator

The purpose of this email is to clarify what steps you can take to protect your privacy and identity, provide transparency about the incident, and outline steps the university is taking.

What steps should you take?

At this time your SFU account has not been compromised, nor have we found evidence of compromised passwords, banking information, or regulated data (such as Social Insurance Numbers).

However, due to the type of personally identifiable information exposed you may be at an increased risk for:

- Third-party profile building
- Unsolicited bulk or commercial email
- Identity theft

We recognize how frustrating it may be for individuals who had their personally identifiable information exposed. Although the risk of identity theft is low, we recommend that you monitor personal accounts and memberships of all kinds for any unusual activity over the next several months.

If you are a current user of SFU systems, we encourage you to ensure that you are using Multifactor Authentication (MFA). During this time when work and study from home has increased, attackers are using increasingly sophisticated ways to obtain passwords. MFA is one of your best defenses against remote attacks. To ensure account security, all faculty and staff will be required to enroll in MFA by May 2021, and all students during the fall 2021 term.

If you are a current faculty or staff at the university, please also ensure you connect to SFU's Virtual Private Network (VPN) to encrypt and secure your connection while working remotely.

What steps is SFU taking?

SFU is currently notifying all individuals impacted by this breach and assisting those who may have questions or need assistance. Additionally, the university is:

- Continuing to conduct a full forensic analysis
- Coordinating with the Office of the Information and Privacy Commissioner (OIPC) for B.C.
- Auditing internal policies and procedures to identify improvements
- Accelerating initiatives that continue strengthening our cyber-security systems

(the "**SFU Incident Summary**")

SFU's Misconduct

6. SFU's extensive access, receipt, collection, use, storage, transfer or transmission of the Personal Information made it foreseeable to SFU that its electronic databases are a prime target for criminal activity including attempts to hack and steal the Personal Information.

7. On February 28, 2020, SFU was the subject of a ransomware attack, which also resulted in a data breach exposing personal information. Notwithstanding this, SFU failed to take reasonable steps to strengthen its cybersecurity and to protect the Personal Information accessed in the Data Breach. Instead, SFU stored the Personal Information on an unencrypted spreadsheet, exposing it to easy access by cybercriminals.

8. As a university collecting and retaining highly-sensitive information, SFU was aware at all material times of its obligation to protect user information, including the Personal

Information, from unauthorized access by third parties. The Personal Information, alone or in combination, is deserving of protection.

9. At all material times, SFU failed to handle the collection, retention, protection, security and disclosure of the Personal Information in accordance with the standards imposed by the *Personal Information Protection Act*, SBC 2003, c 63 ("***PIPA***") and related enactments, and the *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5 ("***PIPEDA***").

10. At all material times, SFU failed to make reasonable security arrangements to prevent loss, theft and unauthorized access, collection, use, disclosure, copying, modification or disposal of the Personal Information.

11. At all material times, SFU failed to implement physical, organizational or technological safeguards or control procedures to prevent loss, theft and unauthorized access, collection, use, disclosure, copying, modification or disposal of the Personal Information.

12. At all material times, SFU failed to use organizational or technological safeguard measures to protect the Personal Information, or used measures that were outdated and inadequate having regard to the sensitivity of the Personal Information.

13. At all material times, SFU failed to hire competent employees, failed to properly supervise its employees, or failed to provide proper training to its employees.

14. In the alternate, SFU failed to exhibit sufficient skill, competence, and due diligence in the hiring or contracting with outside information technology and/or data services.

15. At all material times, SFU failed to employ ongoing monitoring and maintenance that would adequately identify and address evolving digital vulnerabilities and threats.

16. At all material times, SFU failed to detect loss, theft, and unauthorized access, collection, use, disclosure, copying, modification or disposal of the Personal Information, adequately or at all.

17. Following the Data Breach, SFU failed to immediately notify the Plaintiff and other Class Members that their Personal Information had been left unprotected and subjected to loss, theft,

unauthorized access, collection, use, disclosure, copying, modification or disposal. SFU made this choice to delay disclosure to current and former faculty, staff and students wilfully and deliberately.

18. SFU has failed to provide any means for Class Members to determine the extent to which their Personal Information was subject to loss, theft, and unauthorized access, collection, use, disclosure, copying, modification as a result of the Data Breach.

Harm to the Plaintiff and Class Members

19. The Plaintiff and Class Members have suffered loss and damages because of the Data Breach, including but not limited to:

a. Violation of privacy;

b. Psychological distress;

c. Costs incurred in preventing identity theft;

d. Costs incurred in paying for credit monitoring services;

e. Out-of-pocket expenses;

f. Wasted time, inconvenience, frustration, and anxiety associated with taking precautionary steps to reduce the likelihood of identity theft or improper use of credit information, and to address the credit flags placed on their credit files;

g. Time lost engaging in precautionary communications with third parties such as credit card companies, credit agencies, banks, and other parties to inform them of the potential that their Personal Information may be misappropriated and to resolve delays caused by flags placed on their credit files; and

h. A possibility of exposure to future false marketing by cybercriminals fictitiously holding themselves out SFU, thereby subjecting Class Members to further identity and information theft in the future.

Part 2: RELIEF SOUGHT

20. An order certifying this action as a class proceeding under the *Class Proceedings Act*, RSBC 1996, c 50;

21. General damages for the tort of negligence;

22. A declaration that SFU committed a tort under the *Privacy Act*, RSBC 1996, c 373 ("***Privacy Act***");

23. Statutory damages for breach of the *Privacy Act*;

24. General damages for the tort of intrusion upon seclusion;

25. The costs of administering the plan of distribution of the recovery in this proceeding;

26. An order that the Defendant shall offer credit protection services to each Class Member for a period of five years, at the Defendant's cost;

27. Interest under the *Court Order Interest Act*, RSBC 1996, c 79; and

28. Such further and other relief as this Honourable Court may deem just.

Part 3: LEGAL BASIS

29. The Plaintiff pleads and relies on the *Class Proceedings Act*, RSBC 1996, c 50, the *Privacy Act*, *PIPA* and related enactments, *PIPEDA*;

SFU's Statutory Obligations to Canadian Class Members

30. As a non-governmental entity handling personal information while carrying on business in British Columbia, SFU was subject to the provisions of *PIPA.* Section 34 of *PIPA* provides:

> An organization must protect personal information in its custody or under its control by making reasonable security arrangements to prevent unauthorized access, collection, use, disclosure, copying, modification or disposal or similar risks.

31. As a non-governmental entity that transfers personal information, including the Personal Information, across provincial and national borders, SFU was subject to the provisions of *PIPEDA.* Section 5(1) of *PIPEDA* provides:

> Subject to sections 6-9 [none of which apply in the present case], every organization shall comply with the obligations set out in Schedule 1.

32. Schedule 1 to *PIPEDA* consists of "Principles Set Out in the National Standard of Canada Entitled Model Code for the Protection of Personal Information, CAN/CSA – Q830-96". These principles provide, among other things, that:

> 4.3 Principle 3 – Consent
>
> The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.
>
> …
>
> 4.5 Principle 5 – Limiting Use, Disclosure, and Retention
>
> Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfilment of those purposes.
>
> …

4.5.3

Personal information that is no longer required to fulfil the identified purposes should be destroyed, erased, or made anonymous. Organizations shall develop guidelines and implement procedures to govern the destruction of personal information.

…

4.7 Principle 7 – Safeguards

Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

4.7.1

The security safeguards shall protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification. Organizations shall protect personal information regardless of the format in which it is held.

4.7.2

The nature of the safeguards will vary depending on the sensitivity of the information that has been collected, the amount, distribution, and format of the information, and the method of storage. More sensitive information should be safeguarded by a higher level of protection. The concept of sensitivity is discussed in Clause 4.3.4.

4.7.3

The methods of protection should include

...

(b) organizational measures, for example, security clearances and limiting access on a “need-to-know” basis; and

(c) technological measures, for example, the use of passwords and encryption.

4.7.4

Organizations shall make their employees aware of the importance of maintaining the confidentiality of personal information.

(the "**Schedule 1 Obligations**")

33. *PIPEDA* includes notification provisions that require an organization aware of a breach to give timely notice to individuals affected by the breach. Section 10.1 of *PIPEDA* provides:

> Notification to individual
>
> [10.1] (3) Unless otherwise prohibited by law, an organization shall notify an individual of any breach of security safeguards involving the individual's personal information under the organization's control if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to the individual.
>
> …
>
> Time to give notification
>
> (6) The notification shall be given as soon as feasible after the organization determines that the breach has occurred.
>
> Definition of significant harm
>
> (7) For the purpose of this section, significant harm includes bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the credit record and damage to or loss of property.

Negligence

34. SFU owed the Plaintiff and Class Members a duty of care to exercise reasonable care with the collection, use, retention, storage, protection, disclosure and disposition of the Personal Information.

35. The duty of care owed by SFU in relation to the Personal Information is informed by and not less than what is required by s 34 of *PIPA* and the Schedule 1 Obligations, but does not depend on breach of statute.

36. SFU breached the standard of care. Particulars of that breach include, but are not limited to:

a. Failure to handle the collection, retention, protection, security, and disclosure of the Personal Information, in accordance with the standards imposed by *PIPA* and *PIPEDA*, and in accordance with the common law;

b. Failure to make reasonable security arrangements to prevent loss, theft, and unauthorized access, collection, use, disclosure, copying, modification or disposal of the Personal Information;

c. Failure to maintain or alternatively implement physical, organizational and technological safeguards or control procedures to prevent loss, theft, and unauthorized access, collection, use, disclosure, copying, modification or disposal of the Personal Information;

d. Failure to use organizational or technological safeguard measures to protect the Personal Information, or the use of measures that were outdated or inadequate having regard to the sensitivity of the information;

e. Hiring incompetent employees, failing to properly supervise its employees, or failing to provide proper training to its employees;

f. Failure to employ ongoing monitoring and maintenance that would adequately identify and address evolving digital vulnerabilities and threats;

g. Failure to detect loss, theft, and unauthorized access, collection, use, disclosure, copying, modification or disposal of the Personal Information;

h. Failure to immediately notify the Plaintiff and other Class Members that their Personal Information had been left unprotected and subjected to loss, theft, unauthorized access, collection, use, disclosure, copying, modification or disposal;

i. Failure to provide any means for Class Members to determine the extent to which their Personal Information was subjected to loss, theft, and unauthorized access, collection, use, disclosure, copying, modification or disposal.

37. SFU knew or ought to have known that a breach of its duty of care would cause loss and damage to the Class Members. As result of SFU's breach of its duty of care, the Plaintiff and other Class Members suffered loss and damage, including, but not limited to:

a. Psychological distress;

b. Costs incurred in preventing identity theft;

c. Costs incurred in paying for credit monitoring services;

d. Out-of-pocket expenses;

e. Wasted time, inconvenience, frustration, and anxiety associated with taking precautionary steps to reduce the likelihood of identity theft or improper use of credit information, and to address the credit flags placed on their credit files; and

f. Time lost engaging in precautionary communications with third parties such as credit card companies, credit agencies, banks, and other parties to inform them of the potential that the Class Members' Personal Information may be misappropriated and to resolve delays caused by flags placed on Class Members' credit files.

38. In addition, Class Members have suffered or will likely suffer further damages from identity theft because the Personal Information was sold for criminal purposes, including identity theft. It is likely or alternatively there is a real and substantial chance the Personal Information will be used in the future for criminal purposes such as to create fictitious bank accounts, obtain loans, secure credit cards or to engage in other forms of identity theft, thereby causing Class Members to suffer additional damages.

39. Further and more specifically, Class Members have suffered, likely will suffer, or are now subject to a possibility that they will suffer additional losses flowing from false marketing by cybercriminals fictitiously holding themselves out as SFU, with which the Class Members truly and properly have a relationship, thereby subjecting Class Members to further identity and information theft causing additional future harm.

Breach of the Privacy Act

40. The *Privacy Act*, s 1 creates a tort, actionable without proof of damage, where a person, wilfully and without a claim of right, violates the privacy of another.

41. As set out above, SFU has breached the *Privacy Act*. SFU willfully and without a claim of right, violated Class Members' privacy, by failing to protect the Personal Information. SFU made a deliberate choice to employ marginal and insufficient security protections for the Personal Information. SFSFU's failings respecting the Personal Information were not reasonable in the circumstances, having regard to the lawful interests of the Plaintiff and Class Members in that information, and were in breach of s 1 of the *Privacy Act*.

42. Further, between the time when SFU identified the Data Breach on February 5, 2021, and when SFU announced the Data Breach to the Plaintiff and Class Members on February 16, 2021, 11 days had elapsed. SFU's delay in notifying the Plaintiff and Class Members willfully and without a claim of right compromised their privacy by:

a. denying Class Members the knowledge of the scope and extent of the Data Breach as it relates to each individual Class Member;

b. denying Class Members the opportunity to protect their Personal Information; and

c. failing to offer Class Members adequate or any credit protection services, fraud protection, and/or identity theft insurance.

43. The Plaintiff and Class Members are entitled to statutory damages as a result of the breaches in the *Privacy Act*.

Intrusion upon Seclusion

44. It is a tort, actionable without proof of harm, for a defendant to:

a. intentionally or recklessly;

b. invade a plaintiff's private affairs or concerns;

c. without lawful justification;

d. where a reasonable person would regard the invasion as highly offensive, causing distress, humiliation or anguish.

45. SFU willfully and without a claim of right violated Class Members' privacy by recklessly failing to protect the Personal Information. SFU's reckless failings respecting the Personal Information were not reasonable in the circumstances, having regard to the lawful interests of the Plaintiff and Class Members in that information. A reasonable person would regard the resulting invasion of the Plaintiff's and Class Members' privacy as highly offensive, causing distress, humiliation or anguish.

46. Further, SFU delayed notifying the public of the Data Breach. SFU's delay in notifying the Plaintiff and Class Members willfully and without a claim of right compromised their privacy by:

a. denying Class Members the knowledge of the scope and extent of the Data Breach as it relates to each individual Class Member;

b. denying Class Members the opportunity to protect their Personal Information; and

c. failing to offer Class Members any credit protection services, fraud protection, and/or identity theft insurance.

47. These Class Members are entitled to damages as a result of SFU's tortious acts.

Injunction

48. The Plaintiff and Class Members are entitled to an injunction under the *Law and Equity Act*, RSBC 1996, c 253 to require SFU to provide credit protection services for five years at the Defendants' cost.

Jurisdiction

49. An action under the *Privacy Act* must be determined in the Supreme Court of British Columbia (*Privacy Act*, s 4).

Plaintiff's address for service:

Slater Vecchio LLP

1800 - 777 Dunsmuir Street
Vancouver, BC V7Y 1K4

Fax number for service: 604.682.5197

Email address for service: service@slatervecchio.com

Place of trial: Vancouver, BC

The address of the registry is:

800 Smithe Street
Vancouver, BC
V6Z 2E1

Date: March 2, 2021

For: _____

Signature of lawyer for plaintiff
Anthony A Vecchio Q.C.
Slater Vecchio LLP

and

Mathew Good
Mathew P Good Law Corp

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

Part 1: CONCISE SUMMARY OF NATURE OF CLAIM:

This is a claim for damages arising out of Simon Fraser University's breaches of privacy through unauthorised access to user data.

Part 2: THIS CLAIM ARISES FROM THE FOLLOWING:

A personal injury arising out of:

[ ] a motor vehicle accident

[ ] medical malpractice

[ ] another cause

A dispute concerning:

[ ] contaminated sites

[ ] construction defects

[ ] real property (real estate)

[ ] personal property

[x] 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

[ ] a matter not listed here

Part 3: THIS CLAIM INVOLVES:

[x] a class action

[ ] maritime law

[ ] aboriginal law

[ ] constitutional law

[ ] conflict of laws

[ ] none of the above

[ ] do not know

Part 4:

Class Proceedings Act, RSBC 1996, c 50

Personal Information Protection Act, SBC 2003, c 63

Personal Information Protection and Electronic Documents Act, SC 2000, c 5

Privacy Act, RSBC 1996, c 373