No. S-207965
Vancouver Registry

IN THE SUPREME COURT OF BRITISH COLUMBIA

Between

STEFAN WITTMAN

PLAINTIFF

and

BLACKBAUD, INC. AND BLACKBAUD CANADA, INC.

DEFENDANT

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

NOTICE OF CIVIL CLAIM

(Blackbaud – 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. Blackbaud, Inc. is an American software company that provides fundraising, financial, and education data management services to thousands of academic, charitable and socially oriented organizations located in Canada, the United States and the United Kingdom (the "**Client Organizations**"). On July 16, 2020, Blackbaud announced that, in May 2020, an unauthorized party had copied, encrypted and removed the Plaintiff's and Class Members' personal information, including but not limited to their name, age, address, driver's licence details, employment history, credit card information, estimated wealth and identified assets, history of philanthropic and political gift-giving, and spousal identity (collectively the "**Personal Information**") that each had provided to one or more of the Client Organizations, in breach of the Class Members' privacy and reasonable expectations (the "**Data Breach**"). Through this suit, Canadian residents seek to hold Blackbaud accountable for the Data Breach.

The Parties

2. The Plaintiff is a resident of British Columbia. At material times before the Data Breach, he donated money and provided Personal Information to BC Cancer Foundation. BC Cancer Foundation is one of the Client Organizations with a place of business in British Columbia.

3. The defendant Blackbaud, Inc. is incorporated under the laws of Delaware with an address for service at 251 Little Falls Drive, Wilmington, Delaware, USA. Blackbaud, Inc. is publicly traded on the NASDAQ stock exchange and carries on business in the United States, the United Kingdom, and Canada.

4. The Defendant Blackbaud Canada, Inc. is incorporated under the laws of Ontario, with an address for service at 181 Bay Street, Suite 4400, Toronto, Ontario. Blackbaud Canada, Inc. is a subsidiary of the defendant Blackbaud, Inc. (collectively with Blackbaud, Inc., "**Blackbaud**"). Blackbaud Canada Inc. carries on business across Canada, including in British Columbia.

5. Blackbaud's business involves seeking out, collecting, retaining, transmitting, manipulating and organizing Personal Information received from the Client Organizations with which it contracts directly. Blackbaud carries on business with the Client Organizations, including Client Organizations operating in British Columbia and throughout Canada, by managing their data through its specialized data software programs which Blackbaud administers. Many of the Client Organizations are based in British Columbia and themselves do business with residents of British Columbia. Blackbaud maintains and operates data centres in British Columbia that contain the data of Client Organizations and Class Members, and which make it subject to the law and jurisdiction of this province.

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

Blackbaud's Public Disclosure of the Data Breach

7. On July 16, 2020, Blackbaud publicly announced that cybercriminals had stolen a subset of its total data and that Blackbaud had paid the cybercriminals a ransom payment in return for

assurances from the unnamed cybercriminals that they would dispose of the stolen data without further misappropriation. On its website - https://www.blackbaud.com/securityincident - Blackbaud described the situation as follows:

> ***Summary of Incident***
>
> In May of 2020, we discovered and stopped a ransomware attack. In a ransomware attack, cybercriminals attempt to disrupt the business by locking companies out of their own data and servers. After discovering the attack, our Cyber Security team—together with independent forensics experts and law enforcement—successfully prevented the cybercriminal from blocking our system access and fully encrypting files; and ultimately expelled them from our system. Prior to our locking the cybercriminal out, the cybercriminal removed a copy of a subset of data from our self-hosted environment. The cybercriminal did not access credit card information, bank account information, or social security numbers. Because protecting our customers' data is our top priority, we paid the cybercriminal's demand with confirmation that the copy they removed had been destroyed. Based on the nature of the incident, our research, and third party (including law enforcement) investigation, we have no reason to believe that any data went beyond the cybercriminal, was or will be misused; or will be disseminated or otherwise made available publicly. This incident did not involve solutions in our public cloud environment (Microsoft Azure, Amazon Web Services), nor did it involve the majority of our self-hosted environment. The subset of customers who were part of this incident have been notified and supplied with additional information and resources. We apologize that this happened and will continue to do our very best to supply help and support as we and our customers jointly navigate this cybercrime incident.
>
> (the "**Blackbaud Incident Summary**").

8. Blackbaud has not publicly identified the cybercriminals. The basis of Blackbaud's public assurance that the unnamed cybercriminals have returned or destroyed all misappropriated Personal Information has not been explained, much less guaranteed.

Notice to the Plaintiff and Class Members of the Data Breach

9. The Plaintiff received an e-mail on or about July 29, 2020 from BC Cancer Foundation advising that his Personal Information was accessed as a result of the Data Breach. The email from BC Cancer Foundation reiterated the same or similar reassurances stated in the Blackbaud Incident Summary.

10. Each of the Class Members received, or ought to have received, notification correspondence from Blackbaud or a Client Organization that their Personal Information was accessed by unauthorized parties as a result of the Data Breach.

Blackbaud's Misconduct

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

12. As a business operating in the data management sector, Blackbaud 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.

13. At all material times, Blackbaud 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***").

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

15. At all material times, Blackbaud 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.

16. At all material times, Blackbaud 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.

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

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

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

20. Following the Data Breach, Blackbaud 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. Blackbaud made this choice to delay disclosure wilfully and deliberately.

21. Blackbaud 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.

22. Senior officers and directors of Blackbaud were aware at all material times that the Plaintiff and Class Members had a reasonable expectation to be informed of the Data Breach many weeks earlier than July 16, 2020, including being informed of Blackbaud's unlawful conduct in allowing the Data Breach to occur and the nature and extent of Blackbaud's dealings with the cybercriminals. At all material times, Blackbaud's senior officers and directors were aware of Blackbaud's acts and omissions set out herein.

Harm to the Plaintiff and Class Members

23. 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 as the Client Organizations to which the Class Members truly and properly have a relationship with, and thereby subjecting Class Members to further identity and information theft in the future.

Part 2: RELIEF SOUGHT

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

25. General damages for the tort of negligence;

26. A declaration that Blackbaud committed a tort under each of the *Privacy Act BC,* the *Privacy Act SK,* the *Privacy Act MB,* and the *Privacy Act NL*;

27. Statutory damages for breach of the:

a. *Privacy Act BC* for residents of British Columbia;

b. *Privacy Act SK* for residents of Saskatchewan;

c. *Privacy Act MB* for residents of Manitoba;

d. *Privacy Act NL* for residents of Newfoundland & Labrador;

28. General damages for the tort of intrusion upon seclusion for residents of Yukon, Northwest Territories, Alberta, Nunavut, Ontario, New Brunswick, Nova Scotia and Prince Edward Island;

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

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

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

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

Part 3: LEGAL BASIS

33. The Plaintiff pleads and relies on the *Class Proceedings Act*, RSBC 1996, c 50, the *Privacy Act*, RSBC 1996, c 373 ("***Privacy Act***") and related enactments, *PIPA* and related enactments, *PIPEDA*, and the *Court Jurisdiction and Proceedings Transfer Act*, SBC 2003, c 28, ("***CJPTA***").

Blackbaud's Statutory Obligations to Canadian Class Members

34. As a non-governmental entity handling personal information while carrying on business in British Columbia, Blackbaud 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.

35. As a non-governmental entity that transfers personal information, including the Personal Information, across provincial and national borders, Blackbaud 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.

36. 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**")

37. *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

38. Blackbaud 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.

39. The duty of care owed by Blackbaud 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.

40. Blackbaud 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.

41. Blackbaud 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 Blackbaud'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.

42. 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.

43. 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 the Client Organizations to which the Class Members truly and properly have a relationship with, and thereby subjecting Class Members to further identity and information theft causing additional future harm.

Breach of the Privacy Act (BC) and related enactments

44. The *Privacy Act*, RSBC 1996, c 373, 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.

45. As set out above, Blackbaud has breached the *Privacy Act*. Blackbaud willfully and without a claim of right, violated Class Members' privacy, by failing to protect the Personal Information. Blackbaud'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*.

46. Further, between the time when Blackbaud identified the Data Breach at some point in May 2020, the exact date of which is unknown to the Plaintiff but well known to Blackbaud, and when Blackbaud announced the Data Breach to the public on July 16, 2020, approximately six to ten weeks had elapsed. Blackbaud'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, by making public representations that there has been no harm and/or fraud that could be fully traced back to the Data Breach; and

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

47. The Plaintiff and Class Members are entitled to statutory damages as a result of the breaches in the *Privacy Act*. For the same reasons, residents of Saskatchewan are entitled to statutory damages from Blackbaud for breach of *The Privacy Act*, RSS 1978, c P-24; residents of

Manitoba for breach of *The Privacy Act*, CCSM, P125; and residents of Newfoundland & Labrador for breach of the *Privacy Act*, RSNL 1990, c P-22.

Intrusion upon Seclusion

48. For Class Members resident in Ontario and other common law provinces except British Columbia, Saskatchewan, Manitoba and Newfoundland and Labrador, 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.

49. Blackbaud willfully and without a claim of right violated Class Members' privacy by recklessly failing to protect the Personal Information. Blackbaud'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.

50. Further, Blackbaud delayed notifying the public of the Data Breach for a period of weeks or months, the exact extent of the delay being unknown to the plaintiff but well known to Blackbaud. Blackbaud'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, by making public representations that there has been no harm and/or fraud that could be fully traced back to the Data Breach; and

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

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

Injunction

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

Joint and Several Liability

53. The defendants are jointly and severally liable for the actions of and damages allocable to any of them. In the alternative or in addition, Blackbaud is vicariously liable for the actions and omissions of its subsidiaries, affiliates, partners, directors, officers and employees.

Jurisdiction

54. The Plaintiff and Class Members have the right to serve this Notice of Civil Claim on Blackbaud pursuant to the *CJPTA* because there is a real and substantial connection between British Columbia and the facts on which this proceeding is based. This action concerns a tort committed in British Columbia (*CJPTA*, s 10(g)) and a business carried on in British Columbia (*CJPTA*, s 10(h)).

55. 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: August 11, 2020

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.

ENDORSEMENT ON ORIGINATING PLEADING OR PETITION FOR SERVICE OUTSIDE BRITISH COLUMBIA

The plaintiff claims the right to serve this pleading on the defendant Blackbaud outside British Columbia on the ground that the *Court Jurisdiction and Proceedings Transfer Act*, SBC 2003, c 28, s 10 (*CJPTA*) applies because there is a real and substantial connection between British Columbia and the facts on which this proceeding is based. The Plaintiff and Class Members rely on the following grounds, in that this action concerns:

a. a tort committed in British Columbia (*CJPTA*, s 10(g));
b. a business carried on in British Columbia (*CJPTA*, s 10(h))

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

Appendix

Part 1: CONCISE SUMMARY OF NATURE OF CLAIM:

This is a claim for damages arising out of Blackbaud'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