Court File No. VLC-S-S-1810486

No.
Vancouver Registry

In the Supreme Court of British Columbia

Between

BRETT SIPOS

PLAINTIFF

and

NETLINK COMPUTER INC. dba NCIX, ABLE SOLUTIONS INC. AND JOHN DOE CORPORATION

DEFENDANTS

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

NOTICE OF CIVIL CLAIM

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. Netlink Computer Inc. dba "**NCIX**" was a BC-based company that sold computers and peripheral equipment to customers across Canada and the United States. In late 2017, NCIX was assigned into bankruptcy. The Bowra Group Inc. ("**Bowra**") was appointed trustee of the estate. During the bankruptcy process, Bowra engaged Able Solutions Inc. ("**Able**") to dispose of the estate's assets. During that process, Bowra, Able and NCIX's landlord allowed employees' private information, including addresses, social insurance numbers, and other sensitive information, to be exposed and sold to or otherwise obtained by third parties, including criminals. Through this suit, employees seek to hold the defendants accountable for their conduct.

The Parties

2. The defendant NCIX is incorporated pursuant to the laws of British Columbia with an address for service for this proceeding care of The Bowra Group Inc. and a registered address at Suite 550 – North Tower, 5811 Cooney Road, Richmond, BC.

3. The defendant Able Solutions Inc. dba "Able Auctions" is incorporated pursuant to the laws of British Columbia, with an address for service at #5080 – 8171 Akeroyd Road, Richmond, BC. Able carries on business as an auctioneer, including for the disposition of bankrupts' estates.

4. The defendant John Doe Corporation is a corporation that was at material times the owner of the premises at which NCIX carried on business in Richmond, BC (the "**Landlord**"). The identity of the Landlord is presently unknown to the Plaintiff, but is well known to NCIX and Bowra.

5. The Bowra Group Inc. is incorporated pursuant to the laws of Canada and extra-provincially registered in British Columbia, with an address for service 220 – 7565 132nd Street, Surrey, BC. Bowra is a licensed insolvency trustee under the *Bankruptcy and Insolvency Act*, RSC 1985, c B-3. Leave will be sought to bring a claim against Bowra.

6. The Plaintiff, Brett Sipos, is a resident of Surrey, British Columbia. At material times, he was an employee of NCIX. In order to receive his pay cheque and make remittances, he provided private information to NCIX, including his name, address, social insurance number, and other core biographical data, which information alone or in combination is not public information.

7. The Plaintiff brings this claim on his own behalf and on behalf of all former employees of NCIX ("**Class Members**", to be defined in the Plaintiff's application for class certification).

NCIX

8. NCIX was an online computer hardware and software retailer based in Richmond, British Columbia. It had retail outlets in Vancouver, Burnaby, Coquitlam, Richmond and Langley, BC, as well as in Markham, Mississauga, Scarborough and Ottawa, Ontario. NCIX sold to customers in Canada and the United States.

9. NCIX obtained and stored employees' personal information, including social insurance numbers, home addresses, full legal names and other core biographical data, which information alone or in combination is not public information ("**Employees' Private Information**"). The Employees' Private Information was obtained from employees for the limited purpose of paying their salaries, and making necessary government remittances and filings.

10. NCIX stored the Employees' Private Information in physical hardcopy, usually paper, and electronically, including on computer servers (the "**NCIX Servers**").

11. It was an express or implied term of every employee's employment agreement with NCIX that their Private Information would be safeguarded, that it would be retained only so long as necessary for human resources purposes, and that only so much information as was actually required would be collected and retained.

12. The Plaintiff and Class members had direct, transactional relationships with NCIX. The information collected by NCIX was sensitive and collected in the course of its business. It was reasonably foreseeable that harm such as identity theft could result if such information were disclosed or not securely stored, and it was foreseeable to NCIX as an experienced participant in the information technology sector.

The NCIX Bankruptcy

13. On November 21, 2017 NCIX filed a Notice of Intention to Make a Proposal under subsection 50.4(1) of the *Bankruptcy and Insolvency Act* with Bowra being named Proposal Trustee.

14. Subsequently, NCIX did not make a proposal to creditors or seek an extension of the stay under the Notice of Intention to Make a Proposal and was deemed to have filed an assignment in bankruptcy on December 22, 2017. Bowra was appointed trustee of the bankrupt estate under the *Bankruptcy and Insolvency Act*.

15. Upon becoming trustee of NCIX, Bowra took possession of all property and made an inventory of NCIX's property, under the *Bankruptcy and Insolvency Act*, s. 16(3). Bowra was a receiver at law for the purpose of acquiring and retaining the property of NCIX, under the *Bankruptcy and Insolvency Act*, s 16(4).

16. In its capacity as trustee, Bowra took possession of and obtained effective control and responsibility for the Employees' Private Information, including the physical hardcopies and the NCIX Servers.

NCIX's Lack of Due Care

17. While it was still a going concern and upon beginning procedures under the *Bankruptcy and Insolvency Act*, NCIX did not take necessary or appropriate precautions to secure the Employees' Private Information. NCIX failed to properly secure the Employees' Private Information in its control *inter alia* by failing to secure, encrypt, and protect information stored on the NCIX Servers to a commercially-reasonable standard or to ensure that it was kept in a safe location.

18. At material times, NCIX took no, or no effective, steps to properly inventory, secure, dispose of, or protect the Employees' Private Information, in physical hardcopy and stored on the NCIX Servers. In particular, NCIX failed to properly secure the NCIX Servers before it handed control of the business to Bowra.

19. The officers and directors of NCIX were at all material times fully aware of, or reckless or willfully blind to, their own wrongdoing. They knew or ought to have known that the Employees' Private Information was not being appropriately handled.

The Improper Disposition of Employees' Private Information

20. Bowra contracted with Able to dispose of the property from NCIX's estate. The particulars of Bowra and Able's arrangement are unknown to the Plaintiff but well known to Bowra and Able. Able acted as Bowra's agent for the purpose of disposing of the property from NCIX's estate, including media containing the Employees' Private Information.

21. Bowra provided Able with media containing the Employees' Private Information.

22. Able arranged to hold a series of sales, including auctions, to dispose of the property from NCIX's estate. The sales were open to members of the public.

23. During the sales, Private Information was stored unsecured on Able's premises. In particular, physical hardcopies of some Employees' Private Information was left in unlocked file boxes on Able's premises. Members of the public were able to see, manipulate, and take away the Employees' Private Information or copies of it, without any interference by Able, and in fact did so. Able took no appropriate steps to protect the Employees' Private Information on its premises. The current location and status of the physical hardcopies containing the Employees' Private Information is unknown to the Plaintiff, but is well known to Bowra and Able.

24. During the sales, some of the NCIX Servers containing the Employees' Private Information were offered for sale by Able.

25. Some of the NCIX Servers containing the Employees' Private Information were sold by Able.

26. Some of the NCIX Servers containing the Employees' Private Information were sold to criminals.

27. Some or all of the NCIX Servers containing the Employees' Private Information were not encrypted. In the alternative, the NCIX Servers were not protected to industry standard and any security protections were insufficient.

28. In addition, NCIX Servers containing Employees' Private Information were not properly stored by NCIX or Bowra and were stolen or otherwise unlawfully taken. Other NCIX Servers containing Employees' Private Information were seized by the Landlord at NCIX's premises in Richmond, and disposed of through Able or on its own account. Those servers ended up in the hands of the same criminals.

29. The criminals who acquired the NCIX Servers sold the data onwards to other criminals, including identity thieves and cyber criminals. The criminals permitted the Employees' Private Information to be copied, transmitted and used for improper purposes. In particular, the criminals offered the Employees' Private Information for sale over Craigslist and sold copies to overseas buyers. Offences have been committed and will be committed in respect of the Employees' Private Information, contrary to the *Criminal Code*, including but not limited to breaches of ss 380 (fraud), 402.2 (identity theft) and 403 (identity fraud).

30. The Private Information of up to 1,800 employees has been compromised.

31. At material times, the defendants took no, or no effective, steps to:

a. properly inventory, secure, dispose of, or protect the Employees' Private Information, in physical hardcopy and stored on the NCIX Servers;

b. seek consent from employees, including the Plaintiff and Class members, sell or transfer their Private Information; or

c. screen purchasers at the sale to ensure that criminals were prevented from obtaining Employees' Private Information.

32. The officers and directors of Bowra and Able were at all material times fully aware of, or reckless or willfully blind to, their own wrongdoing. They knew or ought to have known that the property from NCIX's estate offered for sale included Employees' Private Information. In addition, employees of Able were specifically alerted during the sales that Private Information was unsecured and ought to be protected. Despite that warning, Able took no steps to secure the Employees' Private Information.

33. The information collected by NCIX was sensitive and collected in the course of its business. As experienced administrators and professionals operating within the bankruptcy and insolvency industry, Bowra and Able were aware that employees' information is often included in the property of bankrupts' estates, and that they took responsibility to protect that data when taking custody of a bankrupt's property. The Landlord, as a sophisticated business organisation, was aware that sensitive employee information is often kept on the physical premises of tenants, and that it took responsibility to protect that data when taking custody of a tenant's property. It was reasonably foreseeable that harm such as identity theft could result if such information were disclosed or not securely stored, and it was foreseeable to Bowra and Able as experienced participants in the insolvency industry, and to the Landlord as a business operating in this privacy-aware time. They ought to have had in place comprehensive policies for protection such data, but did not, or their policies did not meet industry standards, or they did not follow their policies.

34. Employees had no notice that the defendants were disposing of their Private Information. The sale or transfer of the Employees' Private Information, or at a minimum the NCIX Servers containing the Employees' Private Information, was unauthorised by employees. Employees did not consent to the sale or transfer of the Employees' Private Information, or at a minimum the NCIX Servers containing the Employees' Private Information.

35. The defendants' decision to sell the Employees' Private Information, or at a minimum the NCIX Servers containing the Employees' Private Information, was planned and deliberate and was made knowing or reckless or wilfully blind to the fact that employees had not consented to, and were not aware of, its sale.

36. The defendants acted for their own benefit.

37. As a result of the sale of defendants' wrongdoing, the Plaintiff and Class members have suffered a loss and violation of privacy. The Plaintiff and Class members have or will suffer losses associated with responding to this wrongdoing and from additional misuse of their Private Information by criminals.

38. The wrongdoing became public on about September 18, 2018, when the *PrivacyFly.com* published a post about it.

39. On September 21, 2018, the RCMP seized some of the NCIX Servers in Richmond, BC. This comes too late to stop the unauthorised distribution and misuse of the Employees' Private Information.

Part 2: RELIEF SOUGHT

40. An order certifying this action as a class proceeding;

41. General damages for the tort of negligence and for breach of contract;

42. In the alternative, waiver of tort;

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

44. Punitive damages;

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

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

Part 3: LEGAL BASIS

47. The Plaintiff pleads and relies on the *Class Proceedings Act*, RSBC 1996, c 34, the *Personal Information Protection Act*, SBC 2003, c 63 ("PIPA"), the *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5 ("PIPEDA"), the *Privacy Act*, RSBC 1996, c 373, and the *Bankruptcy and Insolvency Act*, RSC 1985, c B-3.

The Defendants' Statutory Obligations

48. As non-governmental entities handling personal information, including the Employees' Private Information, while carrying on business in British Columbia, the defendants were subject to the provisions of PIPA. In particular, PIPA, s 34 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."

49. Employee personal information is specifically protected by PIPA, ss 1, 13-20.

50. As non-governmental entities that transfer personal information, including Employees' Private Information, across provincial or national borders, the defendants were subject to the provisions of PIPEDA. Section 5(1) of PIPEDA provides that "[s]ubject to sections 6 to 9, every organization shall comply with the obligations set out in Schedule 1." None of the exceptions in ss 6 to 9 apply here.

51. Employee personal information is specifically protected by PIPEDA, s 4(1)(b).

52. 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 *inter alia* 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...
>
> 4.7.3 The methods of protection should include
>
> > (a) physical measures, for example, locked filing cabinets and restricted access to offices;
> > (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**")

Negligence

53. The defendants owed the Plaintiff and Class members a duty of care to exercise reasonable care with respect to the collection, use, retention, disclosure and disposition of personal data and information.

54. Furthermore, this duty of care in relation to the Employees' Private Information is informed by and not less than the duties imposed by PIPA s 34 and the Schedule 1 Obligations, but does not depend solely on a breach of statute.

55. The defendants breached the standard of care. Particulars include but are not limited to the following:

a. Failure to handle the retention, security, and disposal of Employees' Private Information in accordance 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 Employees' Private Information;

c. Failure to have in place appropriate policies for the handling of Employees' Private Information obtained from bankrupts' estates;

d. Failure to identify that the Employees' Private Information was not property properly sold in a bankruptcy;

e. Failure to obtain consent to sell or transfer the Employees' Private Information;

f. Failure to screen buyers to keep criminals from acquiring the Employees' Private Information;

g. Failure to maintain or alternatively implement physical, organizational and technological safeguards or control procedures to prevent loss, theft, and unauthorised access, collection, use, disclosure, copying, modification or inappropriate disposal of the Employees' Private Information, including proper encryption and deletion of Employees' Private Information from the NCIX Servers before their sale or disposal;

h. Failure to use organizational safeguard measures to protect the Employees' Private Information, or use of measures that were outdated, inadequate having regards to the sensitivity of the information, and below the reasonable standard currently used in the industry;

i. Failure to use technological safeguard measures to protect the Employees' Private Information, or use of measures that were outdated, inadequate having regards to the sensitivity of the information, and below the reasonable standard currently used in the industry;

j. Failure to ensure that employees were aware of the importance of maintaining the confidentiality of the Employees' Private Information;

k. Failing to properly supervise employees or failing to provide proper training to employees in respect of sensitive personal data including the Employees' Private Information;

l. Failure to detect loss, theft, and unauthorized access, collection, use, disclosure, copying, modification or disposal of the Employees' Private Information; and

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

56. The defendants knew or ought to have known that a breach of the duty of care would cause loss or damage to the Plaintiff and Class members.

57. As a result of the breaches of the duty of care set out above, the Plaintiff and Class members have suffered loss and damage including, but not limited to:

a. Damage to credit reputation;

b. Mental 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; and

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 the Class members' Private Information may be misappropriated and to resolve delays caused by flags placed on Class members' credit files.

58. In addition, the Class members have suffered or will likely suffer further damages from identity theft because the Employees' Private Information was sold for criminal purposes, including identity theft. It is likely or alternatively there is a real and substantial chance that these criminals will use the Employees' Private Information 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 the Class Members to suffer additional damages.

Breach of the Privacy Act

59. The *Privacy Act* creates a tort, actionable without proof of damage, where a person, willfully and without a claim of right, violates the privacy of another.

60. As set out above, the defendants have breached the *Privacy Act*. The defendants willfully and without a claim of right, violated consumers' privacy, by failing to protect Employees' Private Information and deliberately permitting it to be inappropriately disposed of through the sale, and by permitting the theft of the NCIX Servers and interference with the physical hardcopies.

61. The defendants' disposition of the NCIX Servers and their failings respecting the Employees' Private Information generally were not reasonable in the circumstances, having regard to the lawful interests of the Plaintiff and Class Members in that information, and was in breach of s 1 of the *Privacy Act*. In addition, or in the alternative, the Employees' Private Information was not property within the meaning of the *Bankruptcy and Insolvency Act*, and was not capable of being transferred to or disposed of by a trustee or its agent, or a landlord acting under the

Commercial Tenancy Act, the *Rent Distress Act* or otherwise in respect of a tenant`s property on a landlord`s premises, and the defendants had no colour of right to it.

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

Breach of Contract

63. It was an express or in the alternative an implied term of each employee's employment agreement with NCIX that their Private Information necessary for paying them and making remittances would be safeguarded, that it would be retained only so long as necessary to process their human resources needs, and that only so much information as was actually required to process their orders would be collected and retained.

64. As set out above, NCIX breached its contractual obligations to its employees, including the Plaintiff and Class members, in its mishandling of the Employees' Private Information. In particular, NCIX's failure to have a comprehensive information security policy, the lack of ongoing monitoring and maintenance, and the storage of an unencrypted or poorly-protected perpetual copy of the Plaintiff and Class members' Employees' Private Information constituted a breach of contract.

Punitive Damages

65. The defendants' misconduct, as described above, was malicious, oppressive and high-handed, and departed to a marked degree from ordinary standards of decent behaviour. It violated the trust and security of employees. The defendants' actions offend the moral standards of the community and warrant the condemnation of the Court such that an award of punitive damages should be made.

Joint and Several Liability

66. The defendants are jointly and severally liable for the actions of and damages allocable to any of them.

Plaintiff's address for service:

Klein Lawyers LLP
1385 W 8th Ave #400
Vancouver, BC V6H 3V9

Place of trial: Vancouver, BC

The address of the registry is:

800 Smithe Street
Vancouver, BC

V6Z 2E1

Date: September 27, 2018

Signature of lawyer for plaintiff

Mathew P. Good	**David A. Klein**
Co-Counsel for the Plaintiff	Co-Counsel for the Plaintiff
Good Barrister	**Klein Lawyers LLP**

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:

This is a claim for damages arising out of the defendants' breaches of privacy through unauthorised disposal and sale of employee 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:

Bankruptcy and Insolvency Act, RSC 1985, c B

Class Proceedings Act, RSBC 1996, c 34

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