Court File No. VLC-S-S-206353

No.

VANCOUVER REGISTRY

IN THE SUPREME COURT OF BRITISH COLUMBIA

BETWEEN:

DARYL JACOBS

PLAINTIFF

AND:

EASYFINANCIAL SERVICES INC., AND GOEASY LTD.

DEFENDANTS

NOTICE OF CIVIL CLAIM

Brought pursuant to the *Class Proceedings Act*, RSBC 1996, c.50

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 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,

(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

The parties

1. The Defendant Easyfinancial Services Inc. is a company duly incorporated pursuant to the laws of Canada, with a registered office located at 33 City Centre Drive, Suite 510, Mississauga, Ontario, L5B 2N5 ("Easyfinancial").EasyFinancial owned at all material times the EasyFinancial located at 20395 Lougheed Highway, Unit 630, Maple Ridge, British Columbia (the "Premises").

2. The Defendant Goeasy Ltd. is a company duly incorporated pursuant to the laws of Canada, with a registered office located at 33 City Centre Drive, Suite 510, Mississauga, Ontario, L5B 2N5 ("Goeasy").

3. The Plaintiff Daryl Jacobs is an individual who resides in Pitt Meadows, British Columbia.

4. On or about May 22, 2018, the Plaintiff entered the Premises. While there, the Plaintiff entered into a loan agreement with both Defendants, whereby he borrowed $7627.99 from the Defendants, and he agreed to pay them a 46.96% annual interest rate on that sum. Contemporaneously with this loan agreement, the Plaintiff purchased from the Defendants a policy of insurance called a "Loan Protection Plan", which provided a death benefit, injury or sickness benefit, critical illness benefit, and involuntary unemployment benefit. The Plaintiff agreed to pay an insurance premium of $45.33 biweekly, extended for 42 months. Contemporaneously with purchasing the loan agreement and insurance policy from the Defendants, the Plaintiff also purchased from the Defendants a credit monitoring service administered by TransUnion of Canada Inc., for a biweekly fee of $8.21, and a Mastercard credit card that generated a variety of fees for the Defendants. Collectively, all these agreements of May 22, 2018 between the Defendants and the Plaintiff will be referred to hereinafter as the "Agreements".

5. The terms of the Agreements required that the Plaintiff submit a great deal of sensitive personal information to the Defendants. The information that was acquired and retained by the Defendants concerned, among other things, the Plaintiff's sensitive personal identity details, email accounts, telephone numbers, his employment, birth date, all his financial and banking relationships, and his insurance matters. Hereinafter, this material will be referred to as the "Personal Information".

6. The Plaintiff brings this action on his own behalf and on behalf of a class of members, the precise number of which is presently only known to the Defendants (the "Class Members"), which is defined as:

> All persons residing in British Columbia who completed either an online or an in-person application for financial services from the Defendants Easyfinancial and/or Goeasy, and whose personal information was contained in physical documents, databases, and/or computer and electronic equipment in possession or control of the Defendants Easyfinancial and/or Goeasy, which was then compromised and/or disclosed to others.

The Goeasy security breach

7. On April 7, 2020, the Plaintiff received an email from Goeasy (the "Email") advising him that there was a security breach at the branch located in Maple Ridge, B.C. on March 22, 2020. The Email stated that the following elements of the Plaintiff's personal information held by Goeasy were impacted:

   (a) Loan agreement;
   (b) Pre-authorized debit form;
   (c) Loan modification agreement; and
   (d) Any general correspondence pertaining to his loan.

8. In the Email, Goeasy advised the Plaintiff that the loan agreement contained his legal name, address, signature, and loan terms, and the pre-authorized debit form contained his bank account number, institution number and transit number.

9. After receiving the Email, the Plaintiff contacted the Premises and was told by an employee that an individual hacked and disabled their alarm system, and stole physical files, computers and video equipment (the "Breach").

10. The Defendants failed to immediately notify the Plaintiff and the Class members of the Breach and theft of Personal Information.

Breach of contract and warranties

11. The Plaintiff and the Class Members made applications to enter into Agreements with the Defendants, which were similar or identical with respect to the collection, retention and disclosure of Personal Information. As part of the Agreements, the Plaintiff and the Class Members were required to complete either an in-person or an online application at www.easyfinancial.com for the Defendants' products and services, which required that the Plaintiff and each Class Member provide the Personal Information to the Defendants.

12. The Agreements include express and implied provisions, and also provisions that must be applied by operation of statute law.

13. Paragraph 13 of the printed form Loan Agreement document that was executed by the Plaintiff and Defendants on May 22, 2018, is entitled, **"PRIVACY"**. This paragraph sets out the specific limits of the scope of the personal information to be acquired and retained by the Defendants, and the limited uses for which that personal information may be applied by the Defendants. The paragraph then incorporates by reference the terms of the Defendants' "Privacy Policy", which may be viewed on the Defendants website at www.easyfinancial.com/privacypolicy (the "Privacy Policy").

14. The Privacy Policy states:

> *goeasy Ltd., its affiliates, subsidiaries (including RTO Asset Management Inc. operating as easyhome and easyfinancial Services Inc. operating as easyfinancial) and franchisees (collectively, "goeasy", "we", "us" or "our"), have provided this Privacy Policy to describe our personal information handling practices, and to assure you of our continuing commitment to take steps to protect all personal information that we handle in the course of commercial activities. "Personal information", as used in this Privacy Policy, means information about an identifiable individual.*

15. The Privacy Policy states:

> *goeasy limits the amount and type of personal information collected to that which is necessary for our identified purposes, and we collect personal information by fair and lawful means.*

16. The Privacy Policy states:

> *goeasy uses reasonable safeguards and other security standards to protect all personal information in its custody and control against loss or theft, as well as unauthorized access, disclosure, copying, use or modification, regardless of the format in which the information is held. Safeguards will vary depending on the sensitivity, format, location, and storage of the personal information. Only authorized employees, agents, partners and third parties who require access to personal information to fulfill their job requirements will have access to personal information.*

17. The Privacy Policy states:

> *goeasy has appointed a Privacy Officer to oversee compliance with this Privacy Policy and applicable privacy laws.*

18. The Plaintiff has never been contacted by the Defendants' Privacy Officer in respect of the Breach.

19. The Plaintiff does not know whether the Defendants have informed the Office of the Privacy Commissioner of Canada.

20. The Plaintiff says that the federal laws of Canada, including the common law, are available to found the Class Members' claims because, among other things:

    (a) the Defendants are federally licensed Canadian financial institutions;

    (b) the Defendants are subject to the Personal Information Protection and Electronic Documents Act, S.C. 2000, c.5 (the "*PIPEDA*"); and

    (c) the Defendants entered into the Agreement with the Plaintiff and the Class Members, whose terms are uniform across Canada in respect of Goeasy's Privacy Policy.

21. With respect to all the pleaded claims, except for the intentional tort of intrusion upon seclusion, the Plaintiff and the Class Members state that the laws of British Columbia apply.

22. In the alternative and with respect to the intentional tort of intrusion upon seclusion, the plaintiff and the Class Members state that the common law of the province where the Plaintiff or Class Member resided at the time of the breach, should apply.

Damages

23. As a result of the Defendants' breach of contract, negligence, breach of confidence and reckless intrusion upon seclusion, as particularized in Part 3 below, the Plaintiff and Class Members suffered damages including, but not limited to:

    (a) Damage to credit reputation;

    (b) Mental distress;

    (c) Costs incurred in preventing identity theft;

    (d) Out of pocket expenses;

    (e) Wasted time, inconvenience, frustration, and anxiety associated with taking precautionary steps to take steps recommended by the Defendants and 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 take the steps recommended by the Defendants and to inform them of the potential that the Plaintiff and Class Members' Personal Information may be misappropriated and to resolve delays caused by flags placed on the Plaintiff and Class Members' credit files.

24. In addition, the Plaintiff and Class Members have suffered or will likely suffer further damages from identity theft because the Personal Information was stolen by criminals for criminal purposes, including identity theft and "phishing". It is likely, or alternatively there is a real and substantial chance, that these criminals will use the Personal 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 Plaintiff and Class Members to suffer damages.

Part 2: RELIEF SOUGHT

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

2. An order appointing the Plaintiff as the representative plaintiff for the class;

3. An interim or permanent order requiring that the Defendants fund credit monitoring services for the Plaintiff and Class Members;

4. A declaration that the Defendants were in breach of warranty and contract;

5. A declaration that the Defendants owed a duty of care to the Plaintiff and Class Members, and breached the standard of care owed to them;

6. A declaration that the Defendants breached the confidence of the Plaintiff and the Class Members;

7. A declaration that the Defendants intruded upon the seclusion of the Plaintiff and the Class Members;

8. General damages;

9. Special and pecuniary damages;

10. Punitive damages;

11. An order for the aggregate assessment of monetary relief and distribution thereof to the Plaintiff and Class Members;

12. Pre- and post-judgment interest; and

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

Part 3: LEGAL BASIS

1. When the Breach occurred, the Defendants lacked a comprehensive information security policy.

2. The Defendants did not implement sufficiently strong safeguards to protect the sensitive personal information of their customers.

3. The Defendants lacked ongoing monitoring and maintenance of their repositories of their customers' sensitive personal information, to identify and address evolving physical and digital vulnerabilities and threats. As a result, the Defendant was incapable of protecting the Plaintiff's Personal Information.

4. If the Personal Information had been stored with sufficiently strong safeguards, then it would not have been compromised.

5. The Defendants failed to immediately notify the Plaintiff and the Class members of the Breach and theft of Personal Information.

Breach of contract and warranty

6. The Agreements contained the express terms described above in Part 1, and the following additional terms:

    (a) The Defendants would comply with all relevant statutory obligations regarding the collection, retention, and disclosure of the plaintiff and Class Members' personal information, including the obligations set out in (collectively, the "Statutes"):

        i. The *PIPEDA*; and

        ii. The *Personal Information Protection Act*, SBC 2003, c.63 (the "*BC PIPA*").

    (b) The Defendants would not collect, retain, or disclose the Plaintiff's and Class Members' personal information except in the manner and for the purposes expressly authorized by the Agreements or the Statutes;

    (c) The Defendants would keep the personal information of the Plaintiff and the Class Members secure and confidential;

(d) The Defendants would take steps to prevent the personal information from being lost, disseminated, or disclosed to unauthorized persons;

(e) The Defendants would not disclose the personal information without consent;

(f) The Defendants would protect the personal information from compromise, disclosure, loss, or theft;

(g) The Defendants would delete, destroy, or not retain the personal information and would not disclose the personal information when the Plaintiff or Class Members no longer required the Defendants' services, except as required by law; and

(h) The Defendants would exercise care and caution in selecting their outside security providers to ensure that the personal information would be protected from compromise, disclosure, or theft.

7. The Agreements offered peace of mind to the Plaintiff and the Class Members that in exchange for applying for the Defendants' products and services, the Personal Information would not be lost, disseminated, or disclosed to unauthorized persons.

8. The Defendants warranted that they would keep the Personal Information secure and confidential, comply with the obligations set out in the Statutes, and would take sufficient steps to prevent the Personal Information from being lost, disseminated, or disclosed to unauthorized persons.

9. *PIPEDA* contains the following provisions:

5. (1) Subject to sections 6 to 9, every organization shall comply with the obligations set out in Schedule 1.

...

SCHEDULE 1

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 fulfillment of those purposes.

4.5.3: Personal information that is no longer required to fulfill 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.

4.7.5: Care shall be used in the disposal or destruction of personal information, to prevent unauthorized parties from gaining access to the information (see Clause 4.5.3).

10. BC *PIPA* contains the following provisions:

34 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 (1) Despite subsection (2), if an organization uses an individual's personal information to make a decision that directly affects the individual, the organization must retain that information for at least one year after using it so that the individual has a reasonable opportunity to obtain access to it.

(2) An organization must destroy its documents containing personal information, or remove the means by which the personal information can be associated with particular individuals, as soon as it is reasonable to assume that

(a) the purpose for which that personal information was collected is no longer being served by retention of the personal information, and

(b) retention is no longer necessary for legal or business purposes.

11. The Defendants also warranted and guaranteed in the Agreements that they were committed to protecting the privacy and security of customer personal information; would ensure personal and financial information is protected, handled with care and secure; and would be responsible for all personal information in their possession and control.

12. The Defendants breached the express or implied terms of the Agreements' warranty and guarantee by:

(a) Recklessly and improperly maintaining, securing, disseminating, disclosing, or releasing the Personal Information of the Plaintiff and the Class Members;

(b) Failing to comply with the obligations set out in the Statutes;

(c) Retaining the Personal Information of Class Members who did not require the Defendants' products or services and who are not the Defendants' customers, and for no proper purpose;

(d) Failing to implement sufficiently strong physical, electronic and operational safeguards for protecting the Plaintiff and Class Members' Personal Information;

(e) Failing to treat security as their most important priority;

(f) Failing to ensure that their premises and electronic data containing Personal Information was secure;

(g) Failing to strictly manage access to their premises and electronic data;

(h) Failing to implement, manage and/or update systems for ongoing monitoring and maintenance to address evolving physical and digital vulnerabilities and threats and specifically to ensure that security was not breached;

(i) Failing to encrypt the breached data containing the Personal Information; and

(j) Failing to destroy the Personal Information of Class Members who applied for financial services, but were rejected by the Defendants or otherwise did not enter into Agreements with the Defendants.

Negligence

13. The Defendants owed the Plaintiff and Class Members a duty of care:

(a) In their handling of Personal Information;

(b) To ensure the Personal Information would be used by the Defendants for limited purposes;

(c) To keep Personal Information secure and to ensure it would not be lost, disseminated, or disclosed to unauthorized persons; and

(d) To implement control procedures to prevent the unauthorized disclosure of their Personal Information.

14. The Plaintiff says that the Defendants breached the standard of care. Particulars of that breach include but are not limited to:

(a) Failure to handle the collection, retention, security and disclosure of the Personal Information in accordance with their established privacy policies and in accordance with the Statutes and in accordance with the common law;

(b) Failure to keep the Personal Information secure and confidential;

(c) Disclosing the Personal Information to the public without obtaining consent;

(d) Failure to protect the Personal Information from compromise, disclosure, loss, or theft:

(e) Failure to use electronic security measures to safeguard the Personal Information, or use of security measures that were outdated, inadequate, and below the reasonable standard currently used in the financial services industry;

(f) Failure to safeguard the Personal Information to the same standards used to protect Class Members' account information;

(g) Failure to take steps to prevent the Personal Information from being lost, disseminated, or disclosed to the public and unauthorized persons;

(h) Failure to delete and destroy the Personal Information of Class Members who were not customers of the Defendants or who ceased to be customers of the Defendants, or after there was no longer a proper purpose for retaining the Personal Information;

(i) Breaches of contract as particularized in paragraph 12 above;

(j) , failing to properly supervise their employees, or failing to provide proper training to their employees;

(k) Failure to exercise caution and care in selecting and supervising their security and technology service providers and vendors;

(l) Arranging for flags to be placed on the credit files of the Plaintiff and the Class Members without their consent, causing the Plaintiff and the Class Members to incur inconvenience and excessive amounts of time, both now and in the future, in respect of applications for all forms of credit.

15. The Defendants knew a breach of their duty of care would cause damage to the Class Members.

Breach of privacy, breach of confidence, and intrusion upon seclusion

16. The Defendants' conduct, as described herein, also resulted in:

    (a) A breach of confidence, because the Class Members gave their Personal Information to the Defendants who misused their Personal Information to the detriment of the Plaintiff and Class Members; and

    (b) A breach of privacy and reckless intrusion upon the seclusion of the Plaintiff and Class Members in their private affairs in a manner that is highly offensive to a reasonable person and is without lawful justification.

17. As a result of the Defendants' breach of contract, negligence, breach of confidence and reckless intrusion upon seclusion, as particularized above, the Plaintiff and Class Members suffered damages including, but not limited to:

    (a) Damage to credit reputation;

    (b) Mental distress;

    (c) Costs incurred in preventing identity theft;

    (d) Out of pocket expenses;

    (e) Wasted time, inconvenience, frustration, and anxiety associated with taking precautionary steps to take the steps recommended by the Defendants, and 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 take the steps recommended by the Defendants and 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.

18. In addition, the Plaintiff and Class Members have suffered or will likely suffer further damages from identity theft because the Personal Information was stolen for criminal purposes, including identity theft and phishing. It is likely or alternatively there is a real and substantial chance that these criminals will use the Personal 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 Plaintiff and Class Members to suffer damages.

Punitive Damages

19. The conduct of the Defendants, as particularized above, was high-handed, outrageous, reckless, wanton, entirely without care, deliberate, callous, disgraceful, willful, and in complete disregard of the rights of the Plaintiff and Class Members, and as such, renders the Defendants liable to pay punitive damages.

20. The Plaintiff pleads and relies on the Statutes.

Plaintiff's address for service:

Hanson & Co.
300 – 1401 Lonsdale Avenue
North Vancouver, B.C.
V7M 2H9

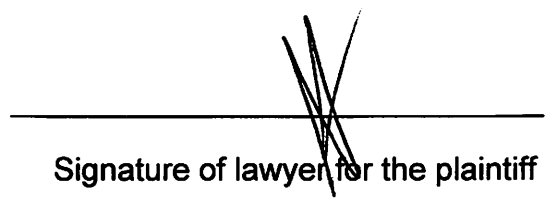
Fax number address for service: **(604) 985-7515**

E-mail address for service: **None**

Place of trial: **Vancouver, British Columbia**

The address of the registry is: **800 Smithe Street**
Vancouver, B.C.
V6Z 2E1 CANADA

Date: June 24, 2020



Signature of lawyer for the plaintiff

JIM HANSON

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:

Proposed class proceeding regarding damages suffered as a result of an information security breach at the defendant financial institution.

Part 2: THIS CLAIM ARISES FROM THE FOLLOWING:

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

[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, R.S.B.C. 1996, c. 34

Personal Information Protection Act, SBC 2003, c 63.