CITATION: Agnew-Americano v. Equifax Canada Co., 2019 ONSC 7110
COURT FILE NO.: CV-17-582551-00CP
DATE: 20191213

SUPERIOR COURT OF JUSTICE - ONTARIO

BETWEEN:	BETHANY AGNEW-AMERICANO and JANE DOE, Plaintiffs
	AND:
	EQUIFAX CANADA CO. AND EQUIFAX, INC., Defendants
BEFORE:	Justice Glustein
HEARD:	September 16, October 8, and October 10, 2019
COUNSEL:	*Jean-Marc Leclerc and Sabrina Callaway*, for the plaintiffs
	Laura Cooper, Sarah Armstrong, Alex D. Cameron, and Pavel Sergeyev, for the defendants

REASONS FOR DECISION

TABLE OF CONTENTS

Contents

CITATION: Agnew-Americano v. Equifax Canada Co., 2019 ONSC 7110
COURT FILE NO.: CV-17-582551-00CP
DATE: 20191213

SUPERIOR COURT OF JUSTICE - ONTARIO

BETWEEN: BETHANY AGNEW-AMERICANO and JANE DOE, Plaintiffs

AND:

EQUIFAX CANADA CO. AND EQUIFAX, INC., Defendants

BEFORE: Justice Glustein

HEARD: September 16, October 8, and October 10, 2019

COUNSEL: *Jean-Marc Leclerc and Sabrina Callaway*, for the plaintiffs

Laura Cooper, Sarah Armstrong, Alex D. Cameron, and Pavel Sergeyev, for the defendants

REASONS FOR DECISION

PART 1: OVERVIEW

[1] I set out a summary of the issues considered at the hearing and in these Reasons.

1.1 Nature of motion

[2] The plaintiff, Alina Owsianik ("Owsianik"),[1] brings a motion under s. 5 of the *Class Proceedings Act, 1992*, S.O. 1992, c. 6 (the "*CPA*")[2] to certify this proposed class action against

---

[1] The current style of cause for the class action maintains Ms. Agnew-Americano and "Jane Doe" as plaintiffs, so I maintain that style of cause for these Reasons. However, only Owsianik is put forward as representative plaintiff.

Ms. Agnew-Americano is not advanced as a proposed representative plaintiff because she was not responsive to attempts to contact her to provide evidence for this motion. The defendants took no position on the request of plaintiff's counsel that Ms. Agnew-Americano be removed as a proposed representative plaintiff and I so order.

Owsianik initially sought to maintain anonymity through the pseudonym "Jane Doe". The defendants opposed certification on that basis. Prior to the hearing, Owsianik agreed to proceed as a named representative plaintiff.

the defendants, Equifax Canada Co. ("Equifax Canada") and Equifax, Inc. ("Equifax US") (collectively, "Equifax").[3]

[3] The claim arises out of the intrusion by unauthorized persons ("hackers") into the Equifax computer systems from May 13, 2017 through July 30, 2017 (the "Data Breach").

[4] Equifax notified approximately 20,000 Canadians that their personal information including names, addresses, and social insurance numbers[4] had been "impacted" and "compromised" by hackers.

[5] Between May 1, 2017 and August 1, 2017, 318,342 persons in Canada had active subscriptions with Equifax for credit monitoring and identity theft protection services.[5]

1.2 The proposed class definition

[6] In her amended notice of motion, Owsianik sought to certify the proposed class action on behalf of:

> (i) all persons in Canada whose personal information was exposed to appropriation by unauthorized persons (i.e. 'hackers') as a result of a security breach occurring between March 7, 2017 and August 1, 2017; and
>
> (ii) all persons in Canada who, between March 7, 2017 and September 7, 2017, purchased from the defendants, their subsidiaries or related companies the following products:
>
> i. Equifax Complete Advantage

Consequently, it is not necessary for me to address the anonymity issue in these Reasons. The pleadings will be amended to provide for Owsianik as the plaintiff.

[2] All references to legislative sections are from the *CPA* unless otherwise noted.

[3] I refer to the collective "Equifax" entities in the singular throughout these Reasons. I note that the parties often refer to "Equifax" in the plural, both in their pleadings and submissions.

[4] (as well as credit card information for 11,670 of that group)

[5] The number of persons in Canada who subscribed to the Subscription Products between March 7, 2017 and July 30, 2017 (the dates that the plaintiff relies upon for subscriber class membership) is not in evidence before the court. That number would necessarily be greater than the 318,342 subscribers in Canada between May 1, 2017 and August 1, 2017.

ii. Equifax Complete Premier,

iii. Equifax Complete Friends and Family, or

iv. any other Equifax products offering credit monitoring and identity theft protection [collectively, "Subscription Products"].

[7] At the outset of the hearing, I advised Owsianik's counsel of my concerns about overlapping between the proposed subclasses. In particular, under the plaintiff's approach, some of the individuals whose data was "exposed to appropriation" by hackers (the proposed first subclass) would also be subscribers to the Subscription Products between March 7, 2017 and September 7, 2017 (the proposed second subclass).

[8] Conversely, some of the subscribers to the Subscription Products between March 7, 2017 and September 7, 2017 (the proposed second subclass) had their data "exposed to appropriation" by hackers (the proposed first subclass).

[9] Consequently, the proposed subclasses would not allow identification of class members, nor be consistent with either (i) the different causes of action relied upon by the plaintiff for each subclass or (ii) the objections of Equifax, all of which depended on an "access" versus "contract" distinction.

[10] At present, there is no evidence to establish a group of additional class members whose personal information was "exposed" but not "accessed". Further, the evidence indicates that "access" occurred from May 13, 2017 to July 30, 2017, and not from March 7, 2017 (the date the vulnerability in the Apache Struts open source application was identified and patched by Apache but not by Equifax).

[11] There was also some confusion as to the proposed end date for subscriber class members. In Owsianik's written submissions (see paras. 72 and 88 of the plaintiff's factum and para. 61 of the plaintiff's reply factum), the plaintiff sought an end date of August 1, 2017 (based on the July 30, 2017 date when Equifax states that the vulnerability was fixed) rather than September 7, 2017 (the date the Data Breach was announced), as sought in her amended notice of motion.

[12] I canvassed the above issues related to the proposed class definition with the parties at the outset of the hearing. The parties then attempted to resolve the class definition prior to the return to court for the second day of the hearing. A draft class definition was circulated by Equifax to the plaintiff and provided to the court at the return of the motion.

[13] The parties agreed on the following aspects of the revised class definition:

(i) the use of "access" (as opposed to "exposed"), "contract-only", and "combined" subclasses,

(ii) the subscriber class members would be those who purchased[6] Subscription Products between March 7, 2017 and July 30, 2017; and

(iii) the end date for those persons whose data was "accessed" would be July 30, 2017.[7]

[14] The only outstanding issue on class definition was whether the dates for "access" would start as of March 7, 2017 or May 13, 2017. Given the evidence I summarize at paragraph 10 above, I held that May 13, 2017 was the appropriate starting date.

[15] For the above reasons, I define the class as follows:

(i) all persons in Canada whose personal information was accessed by hackers as a result of the Data Breach and who did not purchase Subscription Products between March 7, 2017 and July 30, 2017 (the "Access-Only Subclass"),[8]

(ii) all persons in Canada who purchased Subscription Products between March 7, 2017 and July 30, 2017 and whose personal information was not accessed by hackers as a result of the Data Breach (the "Contract-Only Subclass"),[9] and

(iii) all persons in Canada (a) whose personal information was accessed by hackers as a result of the Data Breach and (b) who purchased Subscription Products between March 7, 2017 and July 30, 2017 (the "Combined Subclass").[10]

---

[6] The plaintiff interchangeably refers to the subscriber class members as "subscribers" or those who "purchased subscriptions" during the relevant time period (see paras. 72 and 88 of the plaintiff's factum and para. 61 of the reply factum). Equifax refers to the subscribers as those who "purchased Subscription Products […] that remained active and in force" during the relevant time period (see para. 2 of the Equifax factum). Regardless of the language, the intent of all parties is the same - all persons in Canada who were subscribers to (and, as such, purchased) the Subscription Products during the relevant time period (regardless of when the subscriptions were initially purchased) are included in the subscriber subclasses.

[7] Owsianik proposed August 1, 2017 as the end date for the Data Breach. However, since I use July 30, 2017 as an inclusive end date for the Data Breach, the difference between the August 1, 2017 end date proposed by Owsianik and the July 30, 2017 end date proposed by Equifax is not material.

[8] (an identifiable group constituting less than the approximately 20,000 Equifax customers notified that their personal information was compromised by hackers in the Data Breach)

[9] (an identifiable group constituting less than the total persons in Canada who were subscribers to the Subscription Products between March 7, 2017 and July 30, 2017, but likely greater than 300,000 Equifax customers since at least some of the approximately 20,000 Equifax customers whose data was accessed were not amongst the more than 318,342 subscribers as set out in footnote 5 above)

[16] Under the modified class definition, Owsianik can identify the members of each subclass, without prejudice to later expanding or adding a subclass if required as a result of the litigation process, *e.g.* if the number of individuals whose data was accessed was greater than the notified group, if the dates of access were different, or if there was a separate group of individuals whose personal information was "exposed" (but not "accessed") who may seek additional relief as compared to the Contract-Only Subclass.

[17] Similarly, Equifax can identify the members of each subclass, without prejudice to seeking to modify a subclass as a result of the litigation process, at which point those subscribers could be identified.

[18] Also, the class definition allows the court to address Equifax's objections to (i) the certification of different causes of action relied upon by each of the Access-Only and Combined Subclasses, and (ii) the certification of the Contract-Only Subclass claim in its entirety.

[19] Consequently, the hearing proceeded on the basis of the revised class definition in paragraph 15 above and I rely on that definition in these Reasons.

1.3 Proposed common issues

[20] In her notice of motion, Owsianik sets out 20 proposed common issues (in the singular, "PCI"), listed as numbers (i) to (xx), and attached as Schedule "A" to these Reasons. Owsianik's list sets out all of the PCIs as applying to all class members.

[21] However, counsel for Owsianik acknowledged at the hearing that the applicable causes of action, and therefore the PCIs, differed significantly depending on the particular subclass in question. I summarize the PCIs in relation to each subclass below.

[22] The Access-Only Subclass seeks certification of PCIs based on the claims for negligence (PCIs (i)-(ii)), intrusion upon seclusion (PCIs (iii)-(v)), and breach of provincial privacy legislation (PCIs (vi)-(x)). This subclass does not seek certification of any PCIs arising from the claims in breach of contract or breach of consumer protection legislation.

[23] The Contract-Only Subclass seeks certification of PCIs based on the claims for breach of contract (PCIs (xi)-(xiv)) and breach of consumer protection legislation (PCIs (xv)-(xviii)).[11]

---

[10] (an identifiable group constituting less than the approximately 20,000 Equifax customers notified of their compromised personal information, and when combined with the Access-Only Subclass, forming the total number of Equifax customers notified that their personal information was compromised by hackers in the Data Breach)

[11] The breach of consumer protection legislation claim is based on the *Consumer Protection Act, 2002*, S.O. 2002, c. 30, Sch. A (the "*Consumer Protection Act*"). However, in the alternative that the Ontario legislation is not found applicable to all subscriber class members (the Contract-Only and Combined Subclasses), Owsianik relies on each

This subclass does not seek certification of any PCIs arising from the claims in negligence, intrusion upon seclusion, or breach of provincial privacy legislation.

[24] The Combined Subclass seeks certification of all of the above PCIs.

[25] All of the subclasses seek certification of the PCIs concerning aggregate damages (PCI (xix)) and entitlement to punitive damages (PCI (xx)).[12]

1.4 Equifax objections to certification

[26] Equifax does not oppose certification of the following claims and the corresponding PCIs:

(i) negligence claims of the Access-Only and Combined Subclasses (PCIs (i)-(ii)),

(ii) breach of contract claims by the Combined Subclass (PCIs (xi)-(xiv)),

(iii) breach of consumer protection legislation claims by the Combined Subclass (PCIs (xv)-(xvii)),[13] and

(iv) claims by the Access-Only and Combined Subclasses for entitlement to punitive damages (PCI (xx)).

[27] Equifax objects to certification of the following claims and the corresponding PCIs, based on its submissions that:[14]

(i) The intrusion upon seclusion claim of the Access-Only and Combined Subclasses[15] (from which PCIs (iii) to (v) arise) does not disclose a cause of action under s. 5(1)(a) (the "Intrusion upon Seclusion Objection");[16]

---

of the equivalent provincial and territorial consumer protection legislation, in which case the subscriber subclasses may need to be further subclassified by class member residence. It is not necessary for me to address this issue on the certification motion.

[12] Owsianik initially sought certification of the issue of both quantum of, and entitlement to, punitive damages but at the hearing withdrew the request to certify the quantum issue.

[13] Equifax opposes certification of proposed PCI (xviii) seeking damages or rescission under s. 18 of the *Consumer Protection Act*, as I discuss below.

[14] I do not address in these reasons the initial additional objections of Equifax to (i) the anonymity of the proposed representative plaintiff or (ii) certification of the issue of quantum of punitive damages, as those issues were resolved prior to or during the hearing, as I discuss above.

(ii) The breach of provincial privacy legislation claim of the Access-Only and Combined Subclasses (from which PCIs (vi) to (x) arise) does not disclose a cause of action under s. 5(1)(a) (the "Provincial Privacy Legislation Objection");

(iii) The breach of contract claim of the Contract-Only Subclass (from which PCIs (xi) to (xiv) arise) does not disclose a cause of action under s. 5(1)(a) (the "Breach of Contract Objection");

(iv) The claim of the Contract-Only Subclass under consumer protection legislation (from which PCIs (xv) – (xviii) arise) does not disclose a cause of action under s. 5(1)(a) (the "Consumer Protection Cause of Action Objection");

(v) The claim of the Combined Subclass for rescission or damages under consumer protection legislation (from which PCI (xviii) arises) cannot be certified as a common issue under s. 5(1)(c) (the "Consumer Protection Common Issue Objection"); and

(vi) The claim of all Class Members for an award of aggregate damages (from which PCI (xix) arises) cannot be certified as a common issue under s. 5(1)(c) (the "Aggregate Damages Objection").[17]

[28] The differences between the scope of certification proposed by the parties are significant and can be summarized as follows:

(i) Under the plaintiff's approach:

(a) The Access-Only Subclass can certify claims in negligence, intrusion upon seclusion, and breach of provincial privacy legislation;

(b) The Contract-Only Subclass can certify the breach of contract and consumer protection legislation claims;

---

[15] (*i.e.* those persons whose data was accessed)

[16] The plaintiff does not dispute Equifax's submission that a PCI which does not disclose a cause of action under s. 5(1)(a) cannot be certified as a common issue under s. 5(1)(c) (see *Kalra v. Mercedes-Benz,* 2017 ONSC 3795, at para. 66; *Persaud v. Talon International Inc.*, 2018 ONSC 5377, at para. 137).

[17] Equifax acknowledges that if the intrusion upon seclusion claim is certified, a claim for aggregate damages can be certified as a common issue. Counsel agreed, at the hearing, that if the court found that the intrusion upon seclusion claim disclosed a cause of action, then PCI (xix) could be certified as a common issue "for all or part of the damages claimed".

(c) The Combined Subclass can certify all claims;

(d) All Class Members can seek determination of aggregate damages; and

(e) All Class Members can seek determination of entitlement to punitive damages.

(ii) Under the Equifax approach:

(a) The Access-Only Subclass can only certify the negligence claim;

(b) The Contract-Only Subclass cannot certify any claim and would be removed from the class definition;

(c) The Combined Subclass can only certify the negligence, breach of contract, and consumer protection claims;[18]

(d) Aggregate damages cannot be sought; and

(e) Only those subscribers whose data was accessed (the Access-Only and Combined Subclasses) can seek determination of entitlement to punitive damages.

[29] For the reasons that follow, I reject the objections raised by Equifax.

PART 2: FACTS

[30] There are no contested background facts on this motion. The bulk of the evidence is the same from both parties, based on Equifax's press releases and other public statements which disclosed facts relevant to the Data Breach. Additional evidence filed by the plaintiff was not contested. There were no cross-examinations.

[31] The issues before this court principally relate to s. 5(1)(a). For the purposes of that issue, the pleadings are accepted as true. Consequently, I review the Amended Amended Statement of Claim (the "Claim") below, as the allegations constitute "facts" for the certification motion.

[32] In this section, I review (i) the evidence relevant to the disclosure of the Data Breach and the size of the class, (ii) the evidence relevant to Owsianik, and (iii) the allegations in the Claim.

[18] (without the ability to seek damages or rescission under consumer protection legislation as a common issue)

2.1 Evidence relevant to the Data Breach and the size of the class

[33] The Data Breach was announced on September 7, 2017. Equifax US issued a statement describing an unauthorized intrusion due to a cybersecurity incident by criminals who exploited a U.S. website application vulnerability.

[34] The press release stated that:

(i) Equifax US "today announced a cybersecurity incident" potentially impacting 143 million US consumers and an undisclosed number of Canadian residents;

(ii) "Criminals exploited a U.S. website application vulnerability" to obtain access to "certain files" between mid-May through July 2017;

(iii) The cybersecurity breach involved unauthorized access of Social Security numbers, names, dates of birth, addresses, drivers' licence numbers, credit card numbers and other kinds of personal information;

(iv) Equifax US first discovered the data breach on July 29, 2017; and

(v) Equifax US had set up a dedicated website to help consumers determine if their information was impacted and to sign up for credit file monitoring and identity theft protection.

[35] The Equifax US press release referred to impacted Americans, but also stated that the breach included "unauthorized access to limited personal information for certain UK and Canadian residents." The press release did not set out the number of affected Canadians or refer to a plan to notify them.

[36] On September 15, 2017, Equifax US issued a further press release, in which it explained the method by which hackers accessed Equifax's computer systems. Equifax US stated that:

(i) The attack occurred "through a vulnerability in Apache Struts (CVE-2017-5638), an open-source application framework that supports the Equifax online dispute portal web application";

(ii) The vulnerability was identified and disclosed by the United States Computer Emergency Readiness Team ("US CERT")[19] in March 2017; and

(iii) The hacker intrusions occurred from May 13, 2017 through July 30, 2017.

[19] US CERT is a branch of the US Department of Homeland Security.

[37] The September 15, 2017 press release stated that "the Chief Information Officer and Chief Security Officer are retiring."

[38] On September 19, 2017, Equifax Canada issued a press release, stating that it believed approximately 100,000 Canadian consumers were affected by the breach, but that its investigation was ongoing.

[39] On October 2, 2017, Equifax updated its website to state that the 100,000 "number was preliminary and did not materialize." It stated that the personal information of approximately 8,000 Canadian consumers was "impacted".

[40] In November 2017, Equifax Canada advised, through its website, that in addition to the group of 8,000 "impacted Canadian consumers", a group which "includes 11,670 […] Canadian consumers" had their credit card information impacted, "[as] announced in [Equifax US's] initial statement".

[41] On the November 2017 website page, all consumers were advised that "potentially impacted information includes names, addresses, Social Insurance Numbers, and, in limited cases, credit card numbers" and that "[o]ther potentially impacted information includes username and password, and secret question/secret answer, which we believe are several years old and were login credentials for our direct-to-consumer website".

[42] Equifax sent notification letters to the approximately 20,000 Canadians whose data it had identified as being "impacted" and "compromised" by hackers.

[43] 318,342 persons in Canada had active subscriptions to the Subscription Products between May 1, 2017 and August 1, 2017.[20]

2.2 Facts relevant to Owsianik

[44] Owsianik has been a subscriber to Equifax's Complete Premier Plan since 2013. She remained a subscriber except between September 2015 and November 2016.

[45] Owsianik received a letter from Equifax Canada dated October 17, 2017, confirming that her personal information was "compromised" and "impacted" by hackers. The letter stated the compromised information included Social Insurance Number, name, address, date of birth, phone number, email address, username, password, and secret question/secret answer.

---

[20] The number of subscribers from March 7, 2017 to July 30, 2017 is unknown, but necessarily is greater than the 318,342 subscribers from May 1, 2017 to August 1, 2017, as I discuss at footnote 5 above.

[46] Owsianik agrees to fulfil all of her responsibilities as a representative plaintiff throughout the litigation and has taken appropriate steps to date to assist counsel. She is not aware of having any interest that is in conflict with any other class members on the common issues or issues arising out of them.

2.3 The relevant allegations in the Claim

[47] All of the facts set out below are taken from the Claim. I accept them as true for the purpose of this motion.

2.3(a) The parties

[48] The pleadings with respect to Owsianik (referred to in the Claim as "Jane Doe") set out the information from her affidavit reviewed at paragraphs 44 and 45 above.

[49] Equifax US is an American corporation with its principal place of business in Atlanta, Georgia. Equifax US has global operations or investments in 24 different countries. Equifax US provides credit reporting services and credit protection, fraud management, and credit management services. It does so either directly or indirectly through its operations or through the control of its predecessors, affiliates and subsidiaries, including Equifax Canada.

[50] Equifax Canada is a Canadian corporation with its principal place of business in Toronto. Equifax Canada provides credit reporting services and credit protection, fraud management, and credit management services. Equifax Canada is owned and controlled by Equifax US.

2.3(b) The nature of Equifax's business operations

[51] Equifax operates a business with two aspects that are relevant to this litigation.

[52] A primary aspect of Equifax US's worldwide business operations involves selling credit reporting services for profit. To provide these services, Equifax US and Equifax Canada obtain detailed and sensitive financial information about millions of Canadians and aggregate the information for resale for the purposes of providing credit ratings. Equifax US's global operations organize, assimilate, and analyze data on more than 820 million consumers and more than 91 million businesses worldwide.

[53] Equifax does not obtain the permission of persons whose data it aggregates and stores in its systems. Persons cannot opt out of Equifax's collection of personal information.

[54] Equifax also sells credit protection, fraud management, and credit management subscription services, including identity theft protection. Customers pay Equifax fees in exchange for obtaining protection against credit fraud, identity theft, and other risks involving the unauthorized disclosure of personal information.

2.3(c) The contractual terms

[55] Upon entering into a contractual relationship with its customers for the Subscription Products, Equifax provided subscribers with a Privacy Policy which stated:

> Equifax prides itself on being a trusted steward of personal information and we are committed to protecting the personal information under our control. […][21]
>
> Safeguarding your personal information
>
> Equifax maintains strict security safeguards when storing or destroying your personal information in order to prevent unauthorized access, collection, use, disclosure […] or similar risks. These standards are in place for all information, regardless of how it is stored and we regularly review, test and enhance our systems to ensure they meet accepted industry standards.

[56] It was a term of the contracts that Equifax would maintain strict security safeguards when storing and retaining personal information in order to prevent unauthorized access and similar risks. It was a further term of the contracts that (i) subscribers would be provided with notice if their personal information was disclosed on the internet, and (ii) they would be provided with protection against identity theft.

[57] The contracts between Equifax and its subscribers in Canada provide: "This Agreement is made and will be interpreted under Ontario law, and you submit to the exclusive jurisdiction of Ontario courts located in Toronto."

2.3(d) Other statements and representations by Equifax as to the importance of its information technology ("IT") security

[58] Equifax stated and represented as follows regarding its IT security:

(i) Equifax collected and stored sensitive data, including the potentially identifiable information of customers, and acknowledged that safeguarding this data was "critical" to its "core business operations and strategy";

---

[21] This first sentence from the Privacy Policy is not pleaded but is contained in the Privacy Policy which was in evidence before the court. This passage (along with the balance of the Privacy Policy which was pleaded with excerpts cited below) was relied upon by Owsianik in written and oral submissions at the hearing. In any event, the court on a motion to strike is entitled to review the documents referred to in the pleadings (*Gaur v. Datta*, 2015 ONCA 151, at para. 5).

(ii) Equifax's success was "dependent on its reputation as a trusted steward of information";

(iii) Equifax was a valuable target for cybercriminals due to the vast trove of information it collected;

(iv) Equifax employed "strong data security and confidentiality standards on the data that we provide and on the access to that data" and maintained "a highly sophisticated data information network that includes advanced security, protections and redundancies";

(v) Equifax took "great care to ensure that we use and process personal data in ways that comply with applicable regulations and respects individual privacy";

(vi) Equifax continuously monitored legislative and regulatory activities "in order to remain in compliance" with those laws;

(vii) Equifax had effective internal controls that would provide "reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use or disposition of our assets";

(viii) Equifax used rigorous enterprise risk management programs that targeted its cybersecurity risks, regularly reviewed and updated security protocols, and developed, maintained and enhanced secured proprietary information databases; and

(ix) The CEO of Equifax US stated in August 2017 that "when you have the size database we have, it's very attractive for others to try to get into our database, so it is a huge priority for us as you might guess. [Data security] is my number one worry, obviously."

2.3(e) Additional information about Equifax's conduct after disclosure of the Data Breach

[59] After the September 7, 2017 press release, Equifax US set up a dedicated call centre to assist consumers. In addition, Equifax US stated it would send direct mail notices to persons whose credit card numbers or whose documents containing personal identifying information were impacted.

[60] Equifax US's dedicated website or call centres offered no information to help Canadians determine if they were affected by the Data Breach. While Equifax US's website explained that Canadians were affected by the breach, Equifax Canada's website and its social media accounts had no information regarding the breach. As of the date the statement of claim was first issued, neither defendant offered any way for Canadians to assess whether they were impacted by the

Data Breach, despite one and a half months having passed since Equifax first identified the breach.

[61] By October 13, 2017, Equifax Canada had still not provided notice to Canadians affected by the Data Breach. Equifax Canada only began to notify affected persons as of October 17, 2017, almost three months after the breach was first detected, and over one month after the first public disclosure of the breach.

2.3(f) Specific allegations[22] *relevant to the causes of action pleaded*

2.3(f)(i) Allegations as to Equifax's failure to protect the personal information of the class members

[62] Owsianik pleads serious deficiencies in the Equifax IT security. She alleges:

(a) The defendants' cybersecurity was grossly inadequate and dangerously deficient;

(b) The defendants' data protection measures failed to meet the most basic industry standards;

(c) The defendants failed to implement proper patching protocols;

(d) The defendants failed to encrypt sensitive information;

(e) When encryption was used, the defendants left the keys to unlocking the encryption on public-facing servers;

(f) The defendants failed to encrypt data transmitted over the internet;

(g) The defendants failed to implement adequate authentication measures by using weak passwords and security questions;

(h) The defendants stored sensitive data on public-facing servers and web portals in unencrypted plaintext form, and failed to partition the sensitive information to limit the exposure if a breach occurred;

(i) The defendants used inadequate network monitoring practices by maintaining activity logs and systems to alert when a threat existed, one of the most basic cybersecurity practices;

[22] All allegations set out in section 2.3(f) are quoted *verbatim* from the Claim.

(j) The defendants used outdated and obsolete software;

(k) The defendants allowed unused data to accumulate and failed to dispose of unneeded data;

(l) The defendants failed to restrict access to sensitive data to only those employees whose job responsibilities required such access;

(m) The defendants failed to adequately train its [sic] security personnel;

(n) The defendants failed to perform adequate reviews of its [sic] systems, networks, and security;

(o) The defendants failed to develop a data breach management plan; and

(p) The defendants failed to heed advice by external security experts warning of gross inadequacies in their cybersecurity, including calls to perform comprehensive system reviews.

2.3(f)(ii) Allegations as to Equifax's knowledge that its IT security was inadequate and vulnerable to hackers

[63] Owsianik pleads that Equifax knew its IT security was inadequate and vulnerable to hackers. She alleges:

> The defendants knew their IT security was inadequate and vulnerable to hackers. For example:
>
> (a) In 2014, KPMG performed a security audit of the defendants' IT, which found, among other things, that encryption keys were left on the same public servers where encrypted data was found;
>
> (b) In 2016, Deloitte performed another security audit, which found, among other things, that the defendants had inadequate patching systems; and
>
> (c) In March 2017, Mandiant investigated weaknesses in the defendants' data protection systems in a 'top-secret project' that was personally overseen by Equifax U.S.'s CEO. Mandiant concluded that the defendants' data protection systems were grossly inadequate, and specifically identified the defendants' unpatched systems and misconfigured security policies as indicative of major problems. Instead of heeding Mandiant's advice, the defendants disputed the firm's findings and declined to engage in a broader review of their cybersecurity.

2.3(f)(iii) Allegations with respect to the nature of the personal information accessed in the Data Breach

[64] Owsianik alleges as follows with respect to the personal information accessed in the Data Breach:

> The stolen information are the 'Crown jewels' of personal financial information. The data breach is so sensitive and comprehensive that it allows fraudsters to effect massive financial and personal damage in the form of identity theft and exposure of intimate financial details. These risks will persist many years into the future.

2.3(f)(iv) Allegations with respect to the causes of the breach

[65] Owsianik pleads that:

(i) The Apache Struts vulnerability was described [in the September 15, 2017 press release] as a 'remote code execution attack,' a dangerous type of exploit that allows hackers to force the vulnerable systems into running computer programs written by the attackers, which can make it easy to either steal data or establish a [foothold][23] in the vulnerable system. The weakness was highly dangerous and especially easy to exploit;

(ii) Equifax U.S. and/or Equifax Canada also failed to patch systems containing personal information of Canadian residents in a timely way. Equifax U.S. and/or Equifax Canada failed to maintain strict security safeguards over the personal information of Canadian residents by failing to patch systems; and

(iii) The privacy breach is exacerbated by the fact that: the defendants hold themselves out to the public as data security experts whose very purpose is to protect against data breaches; their inadequate steps taken to respond to the data breaches once discovered; their delay in disclosing the security breach to the public; their inept subsequent efforts to inform and assist affected Canadians; and the fact that the defendants have been involved in previous incidents and failures to guard against unauthorized intrusions into their systems.

[23] The pleading refers to "footnote", but this appears to be a typographical error.

2.3(f)(v) Allegations with respect to the specific causes of action pleaded

2.3(f)(v)(1) Negligence

[66] Owsianik pleads:

(i) The defendants marketed themselves as experts in protecting secure data […];

(ii) In its privacy policy, Equifax U.S. stated that '[w]e have built our reputation on our commitment to deliver reliable information to our customers (both businesses and consumers) and to protect the privacy and confidentiality of personal information about consumers. We also protect the sensitive information we have about businesses. Safeguarding the privacy and security of information, both online and offline, is a top priority for Equifax.' Equifax further stated that '[a]t Equifax, protecting the security of the information in our possession is a responsibility we take very seriously.' Equifax states on its website that 'data and security breaches are scary';

(iii) The defendants breached the standard of care. Particulars include but are not limited to:

(a) the defendants failed to take adequate steps to ensure that a website application vulnerability would not result in the exposure of extremely sensitive personal information belonging to millions of North American consumers;

(b) the defendants failed to apply a website application patch made public in March 2017 in a timely way, waiting until at least August 2017 before applying it;

(c) the defendants failed to detect the unauthorized breaches when they first occurred [sic] mid-May 2017. Cybercriminals were able to access massive amounts of sensitive personal information in Equifax's systems without being detected for approximately six weeks;

(d) subsequent to detecting the existence of the breach on July 29, 2017, Equifax U.S. waited a further 40 days before making a public disclosure of the breach;

(e) after the breach was made public on September 7, 2017, the defendants failed to provide any means for Canadians to determine whether they had been affected by the breach;

(f) the defendants failed to comply with the minimum standards provided in the *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5; and

(g) the defendants failed to give notice to Canadians affected by the breach until October 17, 2017, several months after the breach was detected, and over one month after it was publicly announced.

2.3(f)(v)(2) Breach of contract

[67] The allegations relevant to the terms of the contract are set out at paragraphs 55 to 57 above. Owsianik pleads:

> The defendants breached their contracts with Class Members, exposing their information in a massive cybersecurity breach. The defendants failed to maintain strict security safeguards. The defendants failed to notify Class Members of the cybersecurity breach and failed to protect them against identity theft. The defendants are liable to repay all fees paid by Class Members.

2.3(f)(v)(3) Intrusion upon seclusion

[68] Owsianik pleads that the conduct of Equifax was reckless and intentional, and, as such, constitutes intrusion upon seclusion. Owsianik pleads:

(i) The actions of the defendants constitute intentional or reckless intrusions upon seclusion that would be highly offensive to a reasonable person, for which the defendants are liable. The defendants failed to take appropriate steps to guard against unauthorized access to sensitive financial information involving the Class Members' private affairs or concerns. Their actions were highly offensive, causing distress and anguish to Class Members, for which the defendants are liable and should pay damages; and

(ii) As described above,[24] the actions of the defendants constitute wilful or intentional or reckless intrusions upon seclusion that would be highly

[24] This allegation is made in the "breach of provincial privacy statutes" section of the Claim but is also relevant to the intrusion upon seclusion claim.

> offensive to a reasonable person, for which the defendants are liable. The defendants failed to take appropriate steps to guard against unauthorized access to sensitive financial information involving the Class Members' private affairs or concerns […].

[69] Similarly, Owsianik's allegations as to Equifax's knowledge that its IT security was inadequate and vulnerable to hackers as set out at paragraph 63 above are relevant to the "deliberate" or "reckless" conduct pleaded.

[70] In the "punitive damages" section of the Claim, Owsianik pleads allegations relevant to the alleged "reckless" and "deliberate" conduct of Equifax, and its alleged knowledge of IT security deficiencies. Those allegations are also relevant to the intrusion upon seclusion claim. Owsianik alleges:

> (i) The defendants' conduct was high-handed, reckless, without care, deliberate, and in disregard of Class Members' rights. They knew or ought to have known that their actions and omissions would have a significant adverse effect on all Class Members;
>
> (ii) The defendants knew they had been subject to previous hacking efforts, investigations and audits, that they were particularly vulnerable to being hacked, and knew that their systems were a treasure trove for fraudsters. For example:
>
> (a) In 2004, Equifax confirmed that the records of approximately 1,400 consumers in B.C. and Alberta were accessed by criminals posing as legitimate customers;
>
> (b) In August 2006, the Office of the Privacy Commissioner of Canada audited the personal information management practices of Equifax Canada on the basis that there were reasonable grounds to believe that Equifax Canada was contravening a provision of the *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5;
>
> (c) In 2013, Equifax revealed that hackers had obtained fraudulent access to personal data of celebrities and prominent figures; and
>
> (d) In 2016, Equifax revealed that tax and salary data for hundreds of thousands of employees of a U.S. grocery chain was stolen in a data breach.

2.3(f)(v)(4) Breach of consumer protection legislation

[71] Owsianik alleges:

(i) The defendants engaged in unfair practices by making false, misleading or deceptive representations to Class Members affected by the Equifax Contractual Claims, contrary to the *Consumer Protection Act* and consumer protection statutes in other Canadian provinces […];

(ii) The defendants represented to consumers that they maintained strict security safeguards when storing personal information in order to prevent unauthorized access. In fact, the defendants failed to maintain appropriate or adequate security measures in storing personal information. Although the defendants represented that they are trusted stewards of personal information, the defendants failed to follow basic security procedures by applying software security patches in a timely manner. Contrary to the *Consumer Protection Act* and Equivalent Consumer Protection Statutes, the defendants made false, misleading or deceptive representations that their services had strict security standards that they did not have;

(iii) By making false, misleading or deceptive representations, the defendants engaged in unfair practices, contrary to the *Consumer Protection Act* and Equivalent Consumer Protection Statutes. Consumers affected by the Equifax Contractual Claims are entitled to rescind their contracts and/or an award of damages pursuant to the *Consumer Protection Act* and Equivalent Consumer Protection Statutes; and

(iv) It is not in the interests of justice to require that notice be given pursuant to section 18(15) of the *Consumer Protection Act* (and pursuant to any parallel provisions of the Equivalent Consumer Protection Statutes). The plaintiffs request an order waiving any such notice requirements.

2.3(f)(v)(5) The claim for damages

[72] Owsianik alleges damages "[a]s a result of the defendants' actions". She pleads:

(i) As a result of the defendants' actions, Class Members have suffered and will continue to suffer damages, including:

(a) damages resulting from synthetic or fictitious identity fraud schemes;

(b) damage to credit ratings and perceived credit worthiness;

(c) costs incurred to remedy and prevent identity theft;

(d) damage to reputation;

(e) out-of-pocket expenses;

(f) general damages to be assessed in the aggregate; and

(g) special damages caused by unlawful conduct by third parties, including identity theft, occasioned by or attributable to the defendants' breaches as alleged herein; and

(ii) Damages should be awarded on both an aggregate and individual basis. Equifax Canada has acknowledged that 'synthetic or fictitious identity schemes cost Canadians potentially $1 billion a year in losses. They are real numbers based on carefully calculated cost analysis.' The defendants' acts and omissions, as detailed above, have materially increased the risk to every class member of being victimized by identity theft and have materially increased the quantum of damages that will arise from identify theft to class members.

2.3(f)(v)(6) The claim for punitive damages

[73] The allegations supporting the punitive damages claim are set out at paragraph 70 above.

PART 3: ANALYSIS

[74] I organize my analysis as follows:

(i) I briefly address the general principles relevant to certification;

(ii) I review the applicable test under s. 5(1)(a), since that law is relevant to all of the s. 5(1)(a) objections; and

(iii) I consider each of the Equifax objections summarized at paragraph 27 above.

3.1 General principles relevant to certification

[75] Given the specific objections from Equifax, it is not necessary to set out a detailed analysis of the general principles relevant to certification motions. These principles are not in dispute.

[76] The plaintiff sets out the following submissions, which I adopt:[25]

[25] I do not include all of the citations from the parties' submissions.

(1) THE CERTIFICATION MOTION

Certification is mandatory where the requirements in s. 5(1) of the CPA are met. The CPA is remedial and is to be given a 'generous, broad and purposive interpretation.' The question at certification is whether the action 'can properly proceed as a class action.' Certification does not involve an assessment of the merits and is not intended to be a 'pronouncement on the viability or strength of the action.' The outcome of certification is not predictive of the outcome of the common issues trial.

(2) EVIDENTIARY REQUIREMENTS

Hollick[26] held that plaintiffs must provide 'some basis in fact' for the certification requirements, except the cause of action requirement. *Pro-Sys*[27] affirmed this test and rejected the position that the certification requirements must be proven on a balance of probabilities. *Hollick* does not require some basis in fact for the claim itself, but rather some basis in fact for the certification requirements. The 'some basis in fact' test does not require the court to resolve conflicting facts or evidence. The test reflects the fact that, at certification, the court is 'ill-equipped to resolve conflicts in the evidence or to engage in the finely calibrated assessments of evidentiary weight.' [Emphasis and block letters in original text.]

[77] I also adopt Equifax's submission that:

The Court can only certify an action where, and to the extent that, the would-be representative plaintiff has satisfied *all five* statutory criteria. These criteria are linked; as Ontario courts have observed: 'there must be a cause of action shared by an identifiable class from which common issues arise that can be resolved in a fair, efficient, and manageable way that will advance the proceeding and achieve access to justice, judicial economy, and the modification of behaviour of wrongdoers.'

Subsection 5(1) of the *CPA* was enacted to serve as a meaningful screening device to prevent claims from being prosecuted under a class action procedure if—having regard to the nature of the claims asserted, the surrounding facts and the evidence—the claims are unsustainable in law or are not appropriate for class action treatment. The court is obligated to perform a gatekeeper function,

---

[26] *Hollick v. Toronto (City)*, 2001 SCC 68, [2001] 3 S.C.R. 158 ("*Hollick*")

[27] *Pro-Sys Consultants Ltd. v. Microsoft Corporation*, 2013 SCC 57, [2013] 3 S.C.R. 477 ("*Pro-Sys*")

> scrutinizing the legal basis for the claims and the evidence adduced on the certification motion and, in appropriate cases, refusing to certify the action as a class proceeding. As the Ontario Court of Appeal reaffirmed in *Excalibur Special Opportunities LP v. Schwartz Levitsky Feldman LLP*,[28] '[t]here is no inherent right to proceed on a class basis', and an order certifying the action 'is not the automatic or default outcome of an application for certification of a class action.' [Italics in original text.]

3.2 The applicable law under s. 5(1)(a)

[78] The test under s. 5(1)(a) is the same as on a motion to strike a statement of claim under Rule 21.01(1)(b) of the *Rules of Civil Procedure*, R.R.O. 1990, Reg. 194.

[79] In *Williams v. Canon Canada Inc.*, 2011 ONSC 6571 ("*Williams*"), Strathy J. (as he then was) summarized the principles applicable to the cause of action requirement under s. 5(1)(a) (at para. 176):

> (i) The proper approach is to apply the "plain and obvious" test that is applied on a motion to strike a statement of claim under Rule 21, for failing to disclose a cause of action. There is a very low threshold to prove the existence of a cause of action;
>
> (ii) No evidence is admissible. All allegations of fact pleaded, unless patently ridiculous or incapable of proof, must be accepted as proved and assumed to be true;
>
> (iii) The pleadings will only be struck if it is plain and obvious and beyond doubt that the plaintiff cannot succeed and the action is certain to fail. The novelty of the cause of action will not militate against sustaining the plaintiff's claim. Matters of law which are not fully settled by the jurisprudence must be permitted to proceed; and
>
> (iv) The pleadings must be read generously to allow for drafting inadequacies or frailties and the plaintiff's lack of access to many key documents and discovery information.

(See also *Pro-Sys*, at para. 63)

---

[28] 2016 ONCA 916, 135 O.R. (3d) 743, at para. 105.

[80] The leading case on the law to strike pleadings is *Hunt v. Carey Canada Inc.*, [1990] 2 S.C.R. 959 ("*Hunt*").[29] The Supreme Court of Canada held that the plaintiff (respondent) Hunt could plead that the defendants (appellants), who were involved in the mining of asbestos and the production and supply of a variety of asbestos products, (i) conspired to withhold information concerning the effects of asbestos fibres and (ii) as a result of the conspiracy the plaintiff contracted mesothelioma.

[81] Wilson J. set out several principles governing motions to strike pleadings (quoted *verbatim*):

> (i) *[T]his power of arresting an action and deciding it without trial is one to be very sparingly used [and] our judicial system would never permit a plaintiff to be 'driven from the judgment seat'* in this way without any Court having considered his right to be heard, *excepting in cases where the cause of action was obviously and almost incontestably bad* (*Hunt*, at para. 18, citing *Dyson v. Attorney-General*, [1911] 1 K.B. 410 (C.A.), at 418-19);
>
> (ii) *[T]he fact that the plaintiff's case was a complicated one could not justify striking out the statement of claim. Complex matters that disclosed substantive questions of law were most appropriately addressed at trial where evidence concerning the facts could be led and where arguments about the merits of a plaintiff's case could be made* (*Hunt*, at para. 17);
>
> (iii) The requirement that it be 'plain and obvious' that some or all of the statement of claim discloses no reasonable cause of action before it can be struck out, as well as the proposition that *it is singularly inappropriate to use the rule's summary procedure to prevent a party from proceeding to trial on the grounds that the action raises difficult questions*, has been affirmed repeatedly in the last century […] (*Hunt*, at para. 18);
>
> (iv) *If it is plain and obvious that the action is certain to fail because it contains some such radical defect, then the relevant portions of the statement of claim may properly be struck out.* To allow such an action to proceed, even although it was certain to fail, would be to permit the defendant to be 'vexed' and would therefore amount to the very kind of abuse of the court's process that the rule was meant to prevent. *But if there is a chance that the plaintiff might succeed, then that plaintiff should not be 'driven from the judgment seat'. Neither the length and complexity of*

[29] I refer to the Quicklaw version for paragraph citations.

> *the issues of law and fact that might have to be addressed nor the potential for the defendant to present a strong defence should prevent a plaintiff from proceeding with his or her case.* Provided that the plaintiff can present a 'substantive' case, that case should be heard (*Hunt*, at para. 21); and
>
> (v) *The fact that the case the plaintiff wishes to present may involve complex issues of fact and law or may raise a novel legal proposition should not prevent a plaintiff from proceeding with his action.* (*Hunt*, at para. 27) [Italics added.]

[82] Wilson J. summarized the test as follows (*Hunt*, at para. 33):

> [A]ssuming that the facts as stated in the statement of claim can be proved, is it 'plain and obvious' that the plaintiff's statement of claim discloses no reasonable cause of action? As in England, *if there is a chance that the plaintiff might succeed, then the plaintiff should not be 'driven from the judgment seat'. Neither the length and complexity of the issues, the novelty of the cause of action, nor the potential for the defendant to present a strong defence should prevent the plaintiff from proceeding with his or her case. Only if the action is certain to fail because it contains a radical defect* ranking with the others listed in Rule 19(24) of the British Columbia Rules of Court *should the relevant portions of a plaintiff's statement of claim be struck out* under Rule 19(24)(a). [Italics added.]

[83] The defendants in *Hunt* submitted that the tort of conspiracy should not be extended "beyond the commercial context" which had been considered by the court in *Canada Cement LaFarge Ltd. v. British Columbia Lightweight Aggregate Inc.*, [1983] 1 S.C.R. 452 ("*Canada Cement LaFarge*"). The defendants submitted that the tort "certainly cannot be invoked in personal injury litigation" (*Hunt*, at para. 45) and relied on a passage from Wilson J. in *Frame v. Smith*, [1987] 2 S.C.R. 99, in which she had questioned the appropriateness of extending the tort of conspiracy outside of the commercial context (*Hunt*, at para. 46). Wilson J. held that as the law was not settled, the conspiracy claim could not be struck. She stated (*Hunt*, at paras. 47-48):

> [T]he defendants contend that it would be equally inappropriate to extend the tort of conspiracy to cover the facts of this case. The difficulty I have, however, is in this appeal we are asked to consider whether the allegations of conspiracy should be struck from the plaintiff's statement of claim, not whether the plaintiff will be successful in convincing a court that the tort of conspiracy should extend to cover the facts of this case. In other words, the question before us is simply whether it is 'plain and obvious' that the statement of claim contains a radical defect.
>
> Is it plain and obvious that allowing this action to proceed amounts to an abuse of process? I do not think so. While there has clearly been judicial reluctance to extend the scope of the [conspiracy] tort beyond the commercial context, I do not

> think that this Court has ever suggested that the tort could not have application in other contexts. […] In my view, it would be highly inappropriate for this Court to deny a litigant […] the opportunity to persuade a court that the facts are as alleged and that the tort of conspiracy should be held to apply on these facts. While courts should pause before extending the tort beyond its existing confines, careful consideration might conceivably lead to the conclusion that the tort has a useful role to play in new contexts.

[84] The defendants in *Hunt* also submitted that unless they intended to harm the plaintiff, no claim in conspiracy could lie. After reviewing the applicable case law as to the intent required, Wilson J. held that the issue was not settled, referring to doctrine which noted that conspiracy claims without actual intent could succeed if defendants act unlawfully, direct the conduct towards the plaintiff and others, and "the likelihood of injury to the plaintiff is known to the defendants or should have been known to them in the circumstances" (*Hunt*, at paras. 35 and 43).

[85] Wilson J. stated that it was not for the court to decide on a pleadings motion whether the existing state of the law is "good law" (*Hunt*, at para. 43).

[86] In summary, the principles from *Hunt* are:

(i) A complex matter that discloses substantive questions of law is most appropriately decided at trial;

(ii) An action will be struck on a pleadings motion only if it is plain and obvious that it will fail because it contains a radical defect;

(iii) The fact that the case raises a novel legal proposition is not a basis to strike the pleading; and

(iv) It is not for the court on a pleadings motion to decide if the existing state of the law is good law.

[87] The above principles set out critical parameters under the s. 5(1)(a) test. A certification motion, just as a Rule 21.01(1)(b) motion, is not the forum to determine what the law should be in novel circumstances or how unsettled existing law should be reconciled.

[88] Under *Hunt*, the court can only strike the claim if the court is certain that the plaintiff cannot succeed. The law must develop on the merits of cases, with a proper evidentiary background for the court to consider the relevant policy issues. Unless the claim is "certain to fail", the claim must proceed.

[89] Similarly, in *Transamerica Life Canada Inc. v. ING Canada Inc.*, (2003), 68 O.R. (3d) 457 (C.A.) ("*Transamerica*"), O'Connor A.C.J.O. held (at para. 39) "[w]here the law in a particular area can be described as 'muddy', the court will not strike that part of the pleading, nor hold that the claim or defence must fail."

[90] Finally, there is some uncertainty in the law under Rule 21 as to whether a moving party must establish binding authority prohibiting a cause of action in order to succeed on a motion to strike. In *Dalex Co. v. Schwartz Levitsky Feldman* (1994), 19 O.R. (3d) 463 ("*Dalex*"), Epstein J. (as she then was) held that such authority was required (at para. 6):

> In order to foreclose the consideration of an issue past the pleadings stage, the moving party must show that there is an existing bar in the form of a decided case directly on point from the same jurisdiction demonstrating that the very issue has been squarely dealt with and rejected by our courts.

[91] In *Brookfield Financial Real Estate Group Ltd. v. Azorim Canada (Adelaide Street) Inc.*, 2012 ONSC 3818, D. Brown J. (as he then was) questioned the test set out in *Dalex*, stating (at para. 29) that "[w]hether the standard is so unambiguously strict may be open to some debate".

[92] It is not necessary for the purposes of these Reasons to resolve the above issue. As I discuss below, it is not certain that the claims which are the subject of Equifax's s. 5(1)(a) objections will fail. Consequently, the lack of binding authority prohibiting the plaintiff's claims, while consistent with the unsettled law, is not determinative.

[93] In class action cases, the principles in *Hunt*, *Williams*, and *Transamerica* carry significant weight. The issues raised by the parties are often complex, with the court asked to extend existing legal principles to novel circumstances or consider novel principles of law. The court on a certification motion should not prevent the law from developing unless the defendant can meet the high bar established under the case law.

3.3 Objection 1: Intrusion upon Seclusion Objection

[94] Equifax submits that it is settled law that the intrusion upon seclusion claim of the Access-Only and Combined Subclasses will fail. I do not agree.

3.3(a) The allegations in the Claim relevant to intrusion upon seclusion

[95] Owsianik pleads that Equifax's conduct in relation to the Data Breach was "reckless" "deliberate", "intentional", or "wilful".

[96] I summarize the allegations with respect to the Data Breach as follows:

(i) Equifax represented that it was a "trusted steward" relying on "strict security safeguards" to protect the personal financial information stored on its database;

(ii) Equifax knew that it was a valuable target for cybercriminals due to the information it collected. Equifax "knew they had been subject to previous hacking efforts, investigations and audits, that they were particularly vulnerable to being hacked, and knew that their systems were a treasure trove for fraudsters";

(iii) Equifax represented that it had effective internal controls regarding prevention or timely detection of unauthorized access to sensitive information;

(iv) Despite Equifax's publicly-stated role, its cybersecurity was grossly inadequate, dangerously deficient, and failed to meet the most basic industry standards using outdated and obsolete software;

(v) Equifax left the keys to unlocking the encryption on public-facing servers and stored sensitive data on public-facing servers;

(vi) Equifax failed to heed advice by external security experts warning of gross inadequacies in its cybersecurity;

(vii) Before the Data Breach, Equifax knew that its IT security was inadequate and vulnerable to hackers, based on reviews from leading consultants who concluded that (a) encryption keys were left on the same public servers where encrypted data was found; (b) Equifax had inadequate patching systems; and (c) Equifax's data protection systems were grossly inadequate;

(viii) Equifax was advised by US CERT of the vulnerability in its system as a result of the Apache Struts application in March 2017, yet the hacker intrusions occurred between May 13, 2017 through July 30, 2017;

(ix) "The Apache Struts vulnerability was described as a 'remote code execution attack', a dangerous type of exploit that allows hackers to force the vulnerable systems into running computer programs written by the attackers, which can make it easy to steal data or establish a [foothold] in the vulnerable system. The weakness was highly dangerous and especially easy to exploit";

(x) Based on the above, Equifax's failure to take appropriate steps to guard against unauthorized access to sensitive financial information constitutes intentional or reckless or wilful intrusions upon seclusion that would be highly offensive to a reasonable person; and

(xi) Equifax's conduct was "deliberate, and in disregard of Class Members' rights". "They knew or ought to have known that their actions and omissions would have a significant adverse effect on all Class Members."

[97] The above facts are taken as true under the *Williams* and *Hunt* analysis.

3.3(b) The decision in Jones

[98] Both parties rely on the leading decision on intrusion upon seclusion of *Jones v. Tsige*, 2012 ONCA 32, 108 O.R. (3d) 241 ("*Jones*"). Consequently, I review the case below.

[99] In *Jones*, the intrusion upon seclusion arose when the defendant (respondent) Tsige, a bank employee, accessed private banking records of the plaintiff (appellant) Jones. Tsige was in a common law relationship with Jones' former spouse, and Tsige accessed the plaintiff's records at least 174 times over a period of four years (*Jones*, at paras. 2 and 4).

[100] Each party brought a motion for summary judgment. The motions court (i) granted Tsige's motion and dismissed Jones' action and (ii) dismissed Jones' motion for judgment. The motions judge held that Ontario law did not recognize the tort of breach of privacy (*Jones*, at paras. 8-11).

[101] On appeal, Sharpe J.A. conducted an extensive review of the law. He held that the tort of intrusion upon seclusion should be adopted into Ontario law. He stated (*Jones*, at para. 65):

> In my view, it is appropriate for this court to confirm the existence of a right of action for intrusion upon seclusion. Recognition of such a cause of action would amount to an incremental step that is consistent with the role of this court to develop the common law in a manner consistent with the changing needs of society.

[102] Sharpe J.A. relied (*Jones*, at para. 40) on the Supreme Court of Canada's decision in *R. v. Dyment*, [1988] 2 S.C.R. 417 ("*Dyment*"), in which La Forest J. stated (*Dyment*, at paras. 17, 22):

> (i) privacy was "[g]rounded in man's physical and moral autonomy," and
>
> (ii) "In modern society, especially, retention of information about oneself is extremely important. We may, for one reason or another, wish or be compelled to reveal such information, but situations abound where the reasonable expectations of the individual that the information shall remain confidential to the persons to whom, and restricted to the purposes for which it is divulged, must be protected".

[103] Sharpe J.A. noted that the law of privacy developed in response to technological change, given "routinely kept electronic databases" that "render our most personal financial information vulnerable". He stated that "technological change has motivated the legal protection of the individual's right to privacy." Sharpe J.A. reviewed the rationale for the tort of inclusion upon seclusion. He stated (*Jones*, at paras. 66-69):

> *Privacy has long been recognized as an important underlying and animating value of various traditional causes of action to protect personal and territorial privacy.* Charter jurisprudence recognizes privacy as a fundamental value in our law and specifically identifies, as worthy of protection, a right to informational privacy that is distinct from personal and territorial privacy.
>
> *For over one hundred years, technological change has motivated the legal protection of the individual's right to privacy.* […] The Internet and digital technology have brought an enormous change in the way we communicate and in

> our capacity to capture, store and retrieve information. *As the facts of this case indicate, routinely kept electronic databases render our most personal financial information vulnerable.* Sensitive information as to our health is similarly available, as are records of the books we have borrowed or bought, the movies we have rented or downloaded, where we have shopped, where we have travelled and the nature of our communications by cellphone, e-mail or text message.
>
> *It is within the capacity of the common law to evolve to respond to the problem posed by the routine collection and aggregation of highly personal information that is readily accessible in electronic form. Technological change poses a novel threat to a right of privacy that has been protected for hundreds of years by the common law under various guises and that, since 1982 and the Charter, has been recognized as a right that is integral to our social and political order.*
>
> *Finally, and most importantly, we are presented in this case with facts that cry out for a remedy.* While Tsige is apologetic and contrite, her actions were deliberate, prolonged and shocking. Any person in Jones' position would be profoundly disturbed by the significant intrusion into her highly personal information. […] *In my view, the law of this province would be sadly deficient if we were required to send Jones away without a legal remedy.* [Italics added.]

[104] Sharpe J.A. then set out the elements of the cause of action: (i) deliberate or intentional conduct on the part of the defendant, "within which I would include reckless"; (ii) "the defendant must have invaded, without lawful justification, the plaintiff's private affairs or concerns"; and (iii) a "reasonable person would regard the invasion as highly offensive causing distress, humiliation or anguish" (*Jones*, at para. 71):

> The key features of this cause of action are, first, that the defendant's conduct must be intentional, within which I would include reckless; second, that the defendant must have invaded, without lawful justification, the plaintiff's private affairs or concerns; and third, that a reasonable person would regard the invasion as highly offensive causing distress, humiliation or anguish. However, proof of harm to a recognized economic interest is not an element of the cause of action. I return below to the question of damages, but state here that I believe it important to emphasize that given the intangible nature of the interest protected, damages for intrusion upon seclusion will ordinarily be measured by a modest conventional sum.

[105] In order to ensure that "this cause of action will not open the floodgates", Sharpe J.A. held (*Jones*, at para. 72):

> These elements make it clear that recognizing this cause of action will not open the floodgates. *A claim for intrusion upon seclusion will arise only for deliberate and significant invasions of personal privacy.* Claims from individuals who are

> sensitive or unusually concerned about their privacy are excluded: *it is only intrusions into matters such as one's financial or health records, sexual practices and orientation, employment, diary or private correspondence that, viewed objectively on the reasonable person standard, can be described as highly offensive.* [Italics added.]

[106] Proof of actual loss is not an element of the cause of action. Sharpe J.A. stated (*Jones*, at para. 71) that "proof of harm to a recognized economic interest is not an element of the cause of action" and added (*Jones*, at para 74):

> As I have indicated, proof of actual loss is not an element of the cause of action for intrusion upon seclusion. However, the question necessarily arises: what is the appropriate approach to damages in cases, like the present, where the plaintiff has suffered no pecuniary loss?

[107] With respect to the determination of damages, Sharpe J.A. stated that a "symbolic" award could be appropriate if the plaintiff does not suffer pecuniary loss. He held (*Jones*, at para. 75):

> Where the plaintiff has suffered no provable pecuniary loss, the damages fall into the category of what Professor Stephen M. Waddams, *The Law of Damages*, loose-leaf (Toronto: Canada Law Book, 2011), at para. 10.50, describes as 'symbolic' and others have labelled as 'moral' damages: see *Dulude v. Canada*, (2000), 192 D.L.R. (4th) 714 at para. 30 (Fed. C.A.). They are awarded 'to vindicate rights or symbolize recognition of their infringement': Waddams, at para. 10.50. I agree with Prof. Waddams' observation that a conventional range of damages is necessary to maintain 'consistency, predictability and fairness between one plaintiff and another'.

[108] Sharpe J.A. fixed damages for intrusion upon seclusion to Jones in the amount of $10,000 (*Jones*, at para. 90).

3.3(c) Overview of the parties' positions

[109] Equifax submits that for those class members whose data was accessed by the hackers,[30] it is settled law that the intrusion upon seclusion claim cannot succeed. Equifax submits that:

[30]As I discuss at paragraphs 22-24 above, the intrusion upon seclusion claim is only advanced by those persons in Canada whose data was accessed by the hackers (the Access-Only and Combined Subclasses) and is not advanced by the Contract-Only Subclass.

(i) It is plain and obvious that because the hackers accessed the information, rather than Equifax, the claim must fail. Equifax, as the party who stored personal information on its database,[31] cannot be liable since it did not "[invade], without lawful justification, the plaintiff's private affairs" (*Jones*, at para. 71);

(ii) Material facts have not been pleaded to satisfy the requirement in *Jones* that the impugned conduct must be "reckless". Equifax submits that it is settled law that "reckless" conduct requires advertent misconduct, and there is no pleading that it intended to cause a hacker attack; and

(iii) Material facts have not been pleaded to satisfy the requirement in *Jones* that the hacker attack was a "significant [invasion] of personal privacy" into "financial […] records […] that, viewed objectively on the reasonable person standard, can be described as highly offensive". Equifax submits that it is settled law that access to the personal information hacked (including social insurance numbers, names and addresses)[32] does not rise to the level of the "significant" and "highly offensive" invasion of personal privacy required under *Jones*.

[110] Owsianik submits that it is not certain that the intrusion upon seclusion claim will fail because:

(i) It is not certain that Equifax cannot be liable for intrusion upon seclusion arising from a hacker attack. The court in *Jones* did not directly address this issue (as the defendant Tsige was the person who accessed the information). Further, comments by the court in *Jones* could be applied to find liability on a Database Defendant[33] for a hacker attack. Courts have certified intrusion upon seclusion claims against Database Defendants for hacker attacks and in other similar cases. In any event, if necessary, the law should be permitted to develop to expand intrusion upon seclusion claims to Database Defendants for hacker attacks;

(ii) It is not certain that the pleadings cannot support a finding of "reckless" conduct on the part of Equifax. The scope of "reckless" conduct was not addressed in *Jones* (as the conduct in *Jones* was intentional). Courts have certified intrusion upon seclusion claims against Database Defendants for alleged reckless conduct

[31] In these Reasons, I refer to a defendant who stores personal information on its database as a "Database Defendant".

[32] (and credit card information for 11,670 class members of the approximately 20,000 notified by Equifax)

[33] See footnote 31 above.

in enabling hacker attacks and in other similar cases. If necessary, the law should be permitted to develop to consider the scope of the reckless conduct requirement under *Jones*.

Further, both case law and academic commentary support that "recklessness" in the civil context should be interpreted in an endogenous manner from criminal law, and proposed tests (which have not yet been settled in the law) could be applied by the court to find reckless conduct by Equifax; and

(iii) It is not settled law that access to information including social insurance numbers, names, addresses, email addresses, and phone numbers, which could be used by hackers to engage in identity theft, could not constitute a "significant invasion of personal privacy" which can be "viewed objectively on the reasonable person standard […] as highly offensive".

Courts have certified cases against Database Defendants for hacker intrusions into databases, accessing similar information as in the present case. Other courts have commented that documents leading to identity theft could constitute the types of records subject to an intrusion upon seclusion claim. If necessary, the law should be permitted to develop to consider whether identity theft information meets the third requirement under *Jones*.

3.3(d) Issue 1: Is it certain that an intrusion upon seclusion claim cannot be brought against Equifax for the hacker attack because Equifax did not access the information?

3.3(d)(i) The decision in Jones

[111] Equifax relies on the passage in *Jones* (at para. 71) that "the defendant must have invaded, without lawful justification, the plaintiff's private affairs or concerns", and submits that it is "plain and obvious" that the "invasion" requirement in *Jones* cannot be met in a data breach caused by hackers. In its factum, Equifax describes itself as "a victim of the subject intrusion, and not its perpetrator", who, as such, cannot be liable.

[112] I do not agree that the law is settled under *Jones* that a Database Defendant, who allegedly recklessly enables a hacker attack to occur, cannot be liable for intrusion upon seclusion.

[113] The decision in *Jones* does not directly address whether intrusion upon seclusion could apply to a Database Defendant who recklessly permits a hacker to access a person's private information. That issue was not before the court.

[114] However, there is commentary in *Jones* which supports the application of intrusion upon seclusion to a Database Defendant for hacker attacks. Sharpe J.A. stated that the law of privacy has developed to protect information stored in "routinely kept electronic databases" that "render

our most personal information vulnerable". Sharpe J.A. discussed "technological change [which] has motivated the legal protection of the individual's right to privacy" (*Jones*, at paras. 66-69). Such passages support Owsianik's submission that it is not "beyond doubt" that the principles in *Jones* could be applied to find a Database Defendant liable for a hacker attack.

[115] The need for the court to consider, on the merits, whether intrusion upon seclusion can be established against Database Defendants for hacker attacks exposing persons to identity theft is also consistent with the comments of Sharpe J.A. (*Jones*, at para. 68) that "[i]t is within the capacity of the common law to evolve to respond to the problem posed by the routine collection and aggregation of highly personal information that is readily accessible in electronic form" since "[t]echnological change poses a novel threat to a right of privacy that has been protected for hundreds of years by the common law under various guises".

[116] Even if the comments in *Jones* could not be applied directly to permit intrusion upon seclusion claims against Database Defendants for hacker attacks, Equifax's submission would at best be similar to the appellants in *Hunt*, who submitted that since the law of conspiracy as set out in *Canada Cement Lafarge* related to the commercial context, it could not apply to personal injury matters. The court in *Hunt* rejected that argument because the court was not certain that the law could not be extended to apply to personal injury matters. The court held that the law should be permitted to develop on the facts and should not be closed down at the pleadings stage.

3.3(d)(ii) Case law in which courts have certified intrusion upon seclusion claims against Database Defendants for hacker attacks and in other similar situations

[117] There is no case law on the merits of whether a Database Defendant who recklessly permits a hacker attack to occur is liable for intrusion upon seclusion. While not necessarily determinative of the s. 5(1)(a) requirement, the lack of any case law on the merits is consistent with (i) the uncertainty arising out of *Jones*, since the issue of the liability of a Database Defendant for a hacker attack was not before the court (as I discuss above), and (ii) case law in which courts have certified intrusion upon seclusion claims against Database Defendants for hacker attacks and in other similar situations, which I now review below.

[118] In *Tucci v. Peoples Trust Company*, 2017 BCSC 1525 ("*Tucci*"), the facts were similar to the present case. Certification was sought against the defendant bank who allegedly had improper cybersecurity which permitted hackers to access personal information of bank customers. The information included "name, address, telephone number, email address, date of birth, Social Insurance Number, and occupation" (*Tucci*, at para. 10).[34]

[34] As I discuss at paragraph 180 below, the personal information accessed in *Tucci* is similar to the personal information accessed in the present case, which was set out in the notification letter to Owsianik as "Social

[119] Masuhara J. held that "the essence of the action" is that the defendant "did not adequately secure personal information […] stored in online databases" (*Tucci*, at para. 2). The court found that the tort of intrusion upon seclusion had been adequately pleaded. Masuhara J. held (*Tucci*, at para. 152):

> While it may be a stretch to call the disclosure here reckless, it is not plain and obvious that this must fail. *It is also a stretch to say that the defendant invaded the plaintiff's private affairs, as that was done by a third party. However, it does not appear plain and obvious to me at this stage that being sufficiently reckless may not result in that conduct in effect being attributed to the defendant. This is a relatively new tort and it should be allowed to develop through full decisions.* [Italics added.]

[120] Equifax submits that *Tucci* was wrongly decided. However, the role of a court on a Rule 21 motion is not to determine if existing law is "good law". Rather, the court must determine whether settled law exists such that the action cannot succeed.

[121] In *Kaplan v. Casino Rama Services Inc.*, 2019 ONSC 2025 ("*Kaplan-Certification*"), Belobaba J. dismissed a motion for certification of a claim based on a hacker attack against the defendant casino's database. The basis for the dismissal was a lack of commonality (an issue which does not arise in the present case) of the information hacked from the defendant's database and posted online.

[122] Belobaba J. held that there was a cause of action for intrusion upon seclusion disclosed by the pleadings, arising from the data breach in the hacker attack (*Kaplan-Certification*, at paras. 28-29) (footnotes omitted):

> ***Intrusion upon seclusion***. I was initially of the view that the intrusion upon seclusion tort, first recognized by the Court of Appeal in *Jones v. Tsige*, was doomed to fail on the facts of this case for one simple reason: it was the hacker, and not the defendants, who invaded the plaintiffs' privacy.
>
> However, given the comments of the B.C. court in *Tucci* and this court in *Bennett* and *Equifax Canada*- that this is a new tort that is still evolving and could conceivably support a claim against defendants whose alleged recklessness in the design and operation of their computer system facilitated the hacker's intrusion - I am not prepared to say that the intrusion upon seclusion claim is plainly and obviously doomed to fail. [Emphasis and italics in original text.]

Insurance Number; Name; Address; Date of Birth; Phone Number; Email Address; Username, Password, and Secret Question/Secret Answer".

[123] In *Bennett v. Lenovo (Canada) Inc.*, 2017 ONSC 1082 ("*Bennett*"), the defendants in a class action brought a motion under Rule 21 to strike the claim in its entirety. Belobaba J. struck the breach of contract claim but dismissed the motion to strike the remaining claims in intrusion upon seclusion, merchantability, and violation of provincial privacy laws.

[124] The intrusion upon seclusion was alleged to have occurred because the defendant computer manufacturer pre-loaded laptops with a program that injected unauthorized advertisements which "allow[ed] hackers […] to collect […] bank credentials, passwords and other highly sensitive information" (*Bennett*, at para. 4).

[125] Belobaba J. did not strike the intrusion upon seclusion claim. He noted that the plaintiff alleged that when installing the program, Lenovo "compromise[d] the security of sensitive personal, financial and otherwise confidential information that is commonly stored on computers and other electronic devices" by allowing hackers "to intercept a user's internet connections […] and collect their bank credentials, passwords and other highly sensitive information" including "confidential personal and financial information" which "exposed the class members to significant risks, including the risk that their personal and financial information will be stolen and sold to third parties for commercial purposes" (*Bennett*, at paras. 18-19).

[126] Equifax submits that because Lenovo installed the program, it engaged in an intentional act as required under *Jones*. However, it is not plain and obvious that the decision of the court in *Bennett* was limited to that basis.

[127] In *Bennett*, Lenovo's unsuccessful motion to strike was brought on a similar basis to the argument made by Equifax in the present case. Lenovo submitted that since it did not access the private information, but only allowed third parties to do so, no claim for intrusion upon seclusion could be brought against it. Lenovo argued in its factum:

> 27. An essential element of this cause of action is that the defendant has undertaken some act which constitutes invasion or intrusion upon the private affairs of the plaintiff.
>
> 28. *There is no allegation that Lenovo did anything to invade the private affairs of any putative class member.* Indeed there is no allegation that the private affairs of any putative class member were in fact invaded by anyone. *The only relevant allegation in the Statement of Claim is the allegation in paragraph 62 that by permitting the software to be installed on computers Lenovo "facilitated access by third parties" to such private affairs.*
>
> 29. It is plain and obvious that the Statement of Claim does not disclose any cause of action for intrusion upon seclusion against Lenovo. [Italics added; underlining in original text.]

[128] In essence, the intrusion upon seclusion claim in *Bennett* was based on allegations that Lenovo exposed its computer users to the risk of hacking, allegations similar to those in the

present case. A defendant who permits exposure to third parties by installing software or permitting software to be installed may not be different from a Database Defendant who allegedly recklessly allows hacking to take place if it knows that its system is grossly deficient and is advised of a high risk of exposure to its clients who store their personal financial information on the database (as alleged in the present case). The law on the issue is not settled.

[129] Consequently, it is not certain that the analysis of Belobaba J. in *Bennett* could not be applied to the present case.

3.3(d)(iii) Dictionary definitions and U.S. case law relied upon by Equifax

[130] Equifax also relies on dictionary definitions of "intrude" and "invade" and U.S. case law to submit that it is certain that Equifax could not be found to have invaded or intruded upon the plaintiff's seclusion. I do not agree.

[131] Dictionary definitions do not constitute settled law on whether a Database Defendant can be liable for intrusion upon seclusion for reckless conduct arising from a hacker attack.

[132] Ontario law is not settled even if a novel issue has been discussed (or is settled) in other jurisdictions. The law of a foreign court on a novel issue can be considered on the merits of a claim but is not settled Ontario law.

3.3(d)(iv) Conclusion on whether it is certain that an intrusion upon seclusion claim cannot be brought against Equifax for the hacker attack because Equifax did not access the information

[133] As I set out above:

(i) The principles in *Jones* could apply to (or be expanded to include) a claim for intrusion upon seclusion against a Database Defendant arising from a hacker attack;

(ii) The decisions in *Tucci* and *Kaplan-Certification* are directly on point on the certification of such claims; and

(iii) It is not certain that the rationale in *Bennett* could not be applied to an intrusion upon seclusion claim against a Database Defendant arising from a hacker attack.

[134] Further, the dictionary definitions and U.S. case law relied upon by Equifax do not establish settled law on the issue.

[135] Consequently, the law is not settled as to whether intrusion upon seclusion can be applied, or should be extended (if required), to impose liability on Equifax if it recklessly enabled a hacker attack on its database.

3.3(e) Issue 2: Is it plain and obvious that the pleadings do not disclose a cause of action for reckless conduct?

[136] I first consider the applicable law as to the "reckless" test and then review the material facts pleaded.

3.3(e)(i) The law as to the requirements for "reckless" conduct for intrusion upon seclusion

[137] Equifax submits that it is settled law that "reckless" conduct under *Jones* requires "intentional" conduct by a defendant to intrude or invade on the plaintiff's private affairs such that *Jones* could not be applied against a Database Defendant for a hacker intrusion unless the Database Defendant intentionally or deliberately participated in the intrusion. Applying such a test, Equifax submits that the material facts pleaded in the Claim cannot support a claim of recklessness.

[138] I do not agree that the law is settled on this issue.

3.3(e)(i)(1) The decision in Jones

[139] The court in *Jones* did not consider the meaning of the term "reckless", as the defendant's conduct in reviewing the banking records was intentional. Consequently, the law as to the scope of "reckless" conduct under *Jones* is not settled.

[140] In deciding to adopt intrusion upon seclusion into Ontario law, the court in *Jones* relied upon a broad policy approach where, on the merits of the case, the court held that (i) there were "facts that cry out for a remedy" and (ii) "the law of this province would be sadly deficient if we were required to send Jones away without a legal remedy" (*Jones*, at para. 69). It is not certain that the court would not take same approach to assess the scope of "reckless" conduct by a Database Defendant which enables a hacker attack, if the court found that the facts "cry out for a remedy" and the law would be "sadly deficient" if no remedy was available.

[141] Consequently, *Jones* is not settled law as to the scope of reckless conduct required for the cause of action.

3.3(e)(i)(2) Cases which have certified claims against Database Defendants arising out of hacker attacks when "reckless" conduct is pleaded

[142] The plaintiff relies on several cases which have certified claims against Database Defendants arising out of hacker attacks, based on the alleged reckless conduct of the Database Defendant in enabling the attack to occur.

[143] The decision in *Tucci* supports a cause of action for intrusion upon seclusion against a Database Defendant, if "reckless" conduct is pleaded. The court expressly held that the issue of whether the bank's conduct in permitting the hacker attack was reckless "may be a stretch", but ought to go to trial so that the law could develop (*Tucci*, at para. 152).

[144] Equifax reiterates that *Tucci* is wrongly decided and should not be followed. Equifax submits that the court in *Tucci* committed the "logical fallacy" of treating "recklessness [as] a degree of negligence". Equifax submits that *Tucci* is wrongly decided because it is allegedly inconsistent with criminal law or other definitions of recklessness. Accordingly, Equifax submits that *Tucci* "ought not to be followed".

[145] However, Equifax's submission is inconsistent with the Rule 21 test under *Hunt*. The role of a court on a Rule 21 motion is to determine whether the law is settled, and not whether the existing law is "good law".

[146] In *Kaplan-Certification*, Belobaba J. held that there was a cause of action for the intrusion upon seclusion claim against the defendant casino for a hacker attack since the plaintiff "alleged [that] recklessness in the design and operation of [the defendant's] computer system facilitated the hacker's intrusion" (*Kaplan-Certification*, at para. 29).

[147] Equifax relies on *Broutzas v. Rouge Valley Health System*, 2018 ONSC 6315 ("*Broutzas*"), and *R. v. John Doe*, 2016 FCA 191, 486 N.R. 223. However, neither of those cases involve intrusion upon seclusion claims against Database Defendants for hacker attacks, and consequently do not support a finding that the law is settled as to the scope of "reckless" conduct in such situations.

3.3(e)(i)(3) The definition of "reckless" in other legal contexts

[148] Equifax seeks to rely on definitions of "recklessness" from criminal law, reckless misrepresentation, and malicious prosecution to submit that it is settled law that the recklessness claim against Equifax cannot succeed since intent is required (as Equifax submits would be required in the other legal contexts). I do not agree.

[149] First, Equifax's reliance on definitions of "recklessness" in other legal contexts is, itself, an indication that the law on the issue is not settled for intrusion upon seclusion.

[150] Second, even the cases relied upon by Equifax outside the civil context do not support a finding that the "recklessness" claim in the present action cannot succeed.

[151] In the criminal context, courts have held that recklessness is established when the accused is "aware that there is a danger that his conduct could bring about the result prohibited by the criminal law [but] nevertheless persists, despite the risk" (*Sansregret v. The Queen*, [1985] 1 S.C.R. 570 at p. 582, as relied upon by Equifax).

[152] It is not certain that the conduct pleaded in the present action could not meet the *Sansregret* test, in that the pleadings, read generously, could support a finding Equifax was "aware that there [was] a danger that [its] conduct could bring about the result [of a hacker attack but] nevertheless persist[ed], despite the risk".

[153] Third, it is not settled law that definitions of terms in criminal law or other contexts should be imported into tort law. To the contrary, the issue is one of significant debate.

[154] The concept of "recklessness" does not have a fixed meaning in tort law. In *Economical Mutual Insurance Company v. Doherty*, 2009 BCSC 959, 76 C.C.L.I. (4th) 89 ("*Doherty*"), Myers J. cited (at para. 24) the English case of *Herrington v. British Railway Board*, [1971] 2 Q.B. 107 (C.A.), at p. 137, aff'd [1972] A.C. 877 (H.L.), for the proposition that "'reckless' is an ambiguous word which may bear different meanings in different contexts." The court concluded that "recklessness is not a term with a fixed meaning in the law of tort" (*Doherty*, at para. 40).

[155] P.H. Osborne, in *The Law of Torts* (5th ed.) (Toronto: Irwin Law, 2015) concludes that case law supports "reckless" conduct in the civil context as not requiring intent, but rather conduct undertaken along the spectrum of negligence, possibly including a gross negligence standard with knowledge of a high likelihood of consequences occurring. Osborne comments:

> […] Negligence is conduct that gives rise to a foreseeable and substantial risk of its consequences. As the likelihood of the consequences increases, the conduct of the defendant may be described first as *grossly negligent* and then as *reckless.* (at p. 264)
>
> […] These concepts [i.e., gross negligence and recklessness] play no significant role in tort law. At common law they are drawn within the umbrella concept of negligence. There are, however, some legislative provisions that require the proof of gross negligence or recklessness in order to establish statutory causes of action. (at p. 264, fn. 1) [Italics in original.]

[156] It is not settled law that the standard for "reckless" conduct in intrusion upon seclusion under the Osborne approach could not be met. It is not plain and obvious that a court could not find recklessness by Equifax "as the likelihood of consequences increases", without requiring a deliberate act by Equifax to invade the plaintiff's private information.

[157] Similarly, in their article (J.A. Henderson Jr. & A. Twerski, "Intent and Recklessness in Tort: The Practical Craft of Restating Law" 54 Vand. L. Rev. 1133 (2001)), the authors refer to an earlier edition of the *Restatement of Torts* than the version relied on by Sharpe J.A. in *Jones*, in which the drafters noted that the definitions of intent and recklessness should not be "adjust[ed]" in tort based on other contexts (cited at p. 1136 of the article) (footnotes omitted):

> [I]ntent and recklessness must be kept endogenous to tort without adjusting for how those elements are conceptualized in nonlegal contexts or in legal contexts other than tort. Thus, […] the fact that 'intent' has a special meaning in criminal statutes, should be irrelevant to the drafter of a *Restatement of Torts*. A *Restatement of Torts* speaks to, and only to, the tort system of which it is a constituent part. Other systems – […] systems of criminal justice, and the like – should be left to conceptualize intent and recklessness on their own, perhaps quite differently.

[158] In her recent article, "Ontario's New Invasion of Privacy Torts: Do They Offer Monetary Redress for Violations Suffered via the Internet of Things", (2018) 8:1 UWO J. Leg. Stud. 3, S.K. Mizrahi comments on the lack of guidance regarding recklessness in *Jones* and notes that reckless conduct could arise when a hacker attack, **"**while not desired, [is] substantially certain to result from the defendant's conduct" (at pp. 28-29) (footnotes omitted):

> *The Jones decision provided very little guidance regarding the recklessness standard's application to the Intrusion [sic] tort*; however, the term is generally conceptualized as having 'both a subjective component (awareness that one is creating a serious and relatively easily avoidable risk of harm to others) and an objective component (one's conduct, assessed objectively, must be negligent),' where the defendant reasonably ought to have foreseen the risk. This standard may therefore be very difficult to prove in the context of interconnected technologies, where the risks are infinite and potentially unforeseeable.
>
> Imputing the intention of hacked corporations regarding the consequences suffered as a result of a data breach may be equally difficult. *The possibility, however, may exist under some circumstances to the extent that 'conduct is also intentional if the consequences, while not desired, are substantially certain to result from the defendant's conduct.'* [citing Osborne]. *While this standard would not make it possible to pursue a corporation for all breaches to their systems by hackers, there are two instances that have potential to satisfy the standard. The first is where companies do not at least conform to accepted cybersecurity industry standards. Enabling hacking by neglecting to meet industry accepted security standards such that systems are riddled with vulnerabilities is sufficiently serious to warrant the same consequences as intentional hacking. The fact that the company is not the one actively intruding on users' personal data should not be used to deny legal recourse to victims of such breaches. It is precisely this type of legal imagination that was implemented in Jones to provide redress for a privacy violation that simply '[cried]*

> *out for a remedy.' The invasions suffered by victims of hackers is another such situation.*
>
> *The second instance whereby a company's conduct might be construed as intentional is when it neglects to notify its users of a known breach to allow for preventative actions to be taken against future intrusions. Although this intentional conduct is not the cause of the initial intrusion, it will likely be responsible for any future intrusions that are substantially certain to occur if users' private information is misused by hackers.* [. . .] [Italics added.]

[159] Consequently, it is not certain that definitions of recklessness from other legal contexts will be applied to the "reckless" requirement in *Jones*.

[160] In the present case, with (i) no settled law as to the meaning of "reckless" in the context of an intrusion upon seclusion claim, (ii) case law and academic commentary that could equate recklessness with conduct arising "[a]s the likelihood of the consequences increases", (iii) case law supporting certification of claims against Database Defendants who allegedly recklessly stored the private information accessed in a hacker attack, and (iv) the law not having yet developed on the merits of this issue, it cannot be said that it is plain and obvious that the claim of reckless conduct against Equifax will fail.

3.3(e)(ii) The material facts pleaded

[161] Equifax submits that the Claim does not set out the material facts for a court to find "reckless" conduct by Equifax, as required under the *Jones* test. I do not agree.

[162] Equifax submits that the conclusory pleading at paragraph 37 of the Claim that "[t]he actions of the defendants constitute intentional or reckless intrusions upon seclusion that would be highly offensive to a reasonable person" does not set out the material facts required to establish recklessness. However, that submission ignores the balance of the allegations in the Claim.

[163] Not only must the pleadings be read "generously" (*Hunt*), but the court must also review the entire pleading to determine the material factual allegations. In *Paton Estate v. Ontario Lottery and Gaming Corporation*, 2016 ONCA 458, 131 O.R. (3d) 273 ("*Paton Estate*"), Pardu J.A. held (at para. 14):

> I recognize that these factual allegations were not always neatly tied to a particular cause of action in the statement of claim. However, that is not fatal on a pleadings motion, provided the material facts are pleaded: *Dean's Standard Inc. v. Hachem*, 2014 ONSC 1977, at para. 14; *McGillvray v. Penman*, 2016 ONSC 1271, at para. 12. See also *Almas v. Spenceley*, [1972] 2 O.R. 429 (C.A.), at p. 433.

[164] In the present case, the plaintiff pleads that Equifax:

(i) "knew their IT security was inadequate and vulnerable to hackers",

(ii) knew from a 2014 KPMG "security audit of [Equifax's] IT … that encryption keys were left on the same public servers where encrypted data was found",

(iii) knew from a 2016 Deloitte security audit that Equifax "had inadequate patching systems",

(iv) knew from a March 2017 "top-secret project" of Mandiant, who "investigated weaknesses in [Equifax's] data protections systems", that Equifax's "data protection systems were grossly inadequate, and specifically identified the defendants' unpatched systems and misconfigured security policies as indicative of major problems",

(v) "disputed [Mandiant's] findings and declined to engage in a broader review of their cybersecurity", and

(vi) "knew that "they were particularly vulnerable to being hacked, and knew that their systems were a treasure trove for fraudsters".

[165] Given the above pleaded knowledge of Equifax's "grossly inadequate" data protection systems, Owsianik pleads the following additional facts in support of her intrusion upon seclusion claim:

(i) In March 2017, Equifax was advised by US CERT of the vulnerability in Apache Struts (which supports the Equifax online dispute portal web application) by an e-mail sent directly to Equifax;

(ii) "The Apache Struts vulnerability was […] a 'remote code execution attack', a dangerous type of exploit that allows hackers to force the vulnerable systems into running computer programs written by the attackers, which can make it easy to either steal data or establish a [foothold] in the vulnerable system. The weakness was highly dangerous and especially easy to exploit";

(iii) Equifax "failed to patch systems containing personal information of Canadian residents in a timely way" and "failed to maintain strict security safeguards over the personal information of Canadian residents by failing to patch systems", when:

a. Equifax's "cybersecurity was grossly inadequate and dangerously deficient";

b. Equifax's "data protection measures failed to meet the most basic industry standards";

c. Equifax "failed to implement proper patching protocols";

d. Equifax "failed to encrypt sensitive information";

e. "When encryption was used, [Equifax] left the keys to unlocking the encryption on public-facing servers",

f. Equifax "failed to encrypt data transmitted over the internet";

g. Equifax "failed to implement adequate authentication measures by using weak passwords and security questions";

h. Equifax "stored sensitive data on public-facing servers and web portals in unencrypted plaintext form, and failed to partition the sensitive information to limit the exposure if a breach occurred";

i. Equifax "used inadequate network monitoring practices by maintaining activity logs and systems to alert when a threat existed, one of the most basic cybersecurity practices";

j. Equifax "used outdated and obsolete software";

k. Equifax "allowed unused data to accumulate and failed to dispose of unneeded data";

l. Equifax "failed to restrict access to sensitive data to only those employees whose job responsibilities required such access";

m. Equifax "failed to adequately train its security personnel";

n. Equifax "failed to perform adequate reviews of its systems, networks, and security";

o. Equifax "failed to develop a data breach management plan"; and

p. Equifax "failed to heed advice by external security experts warning of gross inadequacies in their cybersecurity, including calls to perform comprehensive system reviews".

[166] Given the allegations in the Claim, it is not plain and obvious that the facts alleged could not support reckless conduct, even on the higher threshold under criminal law relied upon by Equifax, since the allegations could support a finding that Equifax was "aware that there is a danger that [its] conduct would bring about the result [but] nevertheless persist[ed], despite the risk" (*Sansregret*, at p. 582).

[167] However, even if that criminal standard could not be met on the pleadings, the numerous other possible definitions of "reckless", which have yet to be considered by the courts and which may be endogenous to intrusion upon seclusion (Henderson & Twerski, at p. 1136) could also be supported, as the facts alleged could establish:

(i) a substantial "likelihood of the consequences" occurring, such that the conduct "may be described first as *grossly negligent* and then as *reckless*" [italics in original] (as discussed by Osborne at p. 264); or

(ii) conduct "[e]nabling hacking by neglecting to meet industry accepted security standards such that systems are riddled with vulnerabilities [being] sufficiently serious to warrant the same consequences as intentional hacking" so that "[t]he fact that the company is not the one actively intruding on users' personal data should not be used to deny legal recourse to victims of such breaches" (as discussed by Mizrahi at p. 28).

[168] Consequently, it is not settled that the material facts pleaded in the Claim could not support a finding of recklessness, particularly as it is uncertain how the scope of that concept will develop in the case law.

3.3(f) Issue 3: Have material facts been pleaded to satisfy the requirement in Jones of a significant invasion of personal privacy that, viewed objectively on the reasonable person standard, can be described as highly offensive?

[169] Equifax submits that it is settled law that access to the information as pleaded in the Claim, including social insurance numbers, names, addresses, date of birth, phone number, and email address[35] cannot constitute a "significant" invasion of "personal privacy", nor an intrusion "that, viewed objectively on the reasonable person standard, can be described as highly offensive", as required under *Jones* (at para. 72).

[170] I do not agree.

3.3(f)(i) The decision in Jones

[171] In *Jones*, the defendant accessed the plaintiff's banking records, including the plaintiff's account balances, account postings, transfers, bill payments, and marital status (see the decision of the motions judge reported at 2011 ONSC 1475, 85 C.C.L.T. (3d) 115, at para. 18).

[35] (and credit card information for 11,670 class members)

[172] The issue of whether access to social insurance numbers, credit card information, and other information including names, address, dates of birth, email addresses, and phone numbers, which taken collectively could lead to identity theft, would be a "significant invasion of personal privacy" that is "offensive" to a "reasonable person" does not arise in *Jones*.

[173] However, the inclusion of identity theft information as a "significant invasion of personal privacy" is consistent with cases relied upon by Sharpe J.A. in *Jones* (at paras. 41-42), referring to "informational privacy", which is defined as "the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others".

[174] Consequently, the decision in *Jones* is not settled law that identity theft information could not be the subject of an intrusion upon seclusion claim.

3.3(f)(ii) The risk that the information accessed in the Data Breach could be used by hackers for identity theft

[175] The risk that the information accessed could be used by hackers for identity theft was addressed by the Privacy Commissioner in the *Investigation into Equifax Inc. and Equifax Canada Co.'s compliance with PIPEDA in light of the 2017 breach of personal information*, 2019 CanLII 35618 (PCC) (at para. 149) (footnotes omitted):

> Although there were variations in what personal information was compromised for affected Canadians, most had at least their names, addresses, dates of birth and social insurance numbers compromised. As discussed in Section 1 of this report, these identifiers, combined, present a real risk of unauthorized use by malicious actors for identity theft. This risk is enduring because these identifiers are often used for the purpose of identity validation, and are relatively permanent. [Underlining in original text.]

[176] Equifax acknowledged the risk of identity theft if the information it stores is disclosed. It defines the term "Identity Theft" for the purposes of its subscriber contracts as follows:

> 'Identity Theft' is when your name, address, social insurance number, debit card, credit card or certain other personally identifiable information is stolen, lost, or otherwise used without your knowledge or approval to commit crimes or other fraud in Canada.

[177] Equifax charged its subscribers a monthly fee to protect against that risk. On its website, Equifax described the risk of a data breach as "scary".

3.3(f)(iii) Review of the case law

[178] Equifax provided no case law holding that intrusion upon seclusion cannot be sought against a Database Defendant who allegedly recklessly enables a hacker attack of personal information which can be used for identity theft.

[179] The plaintiff relies on case law that (i) permits an intrusion upon seclusion claim to be brought on the basis of information accessed by hackers which could result in identity theft or (ii) is consistent with such a conclusion.

[180] In *Tucci*, certification was granted on almost identical information being accessed by hackers (*Tucci*, at para. 10). Equifax submits that the case was wrongly decided on this issue as well. However, whether a case is "good" law is not a basis to strike the claim under a Rule 21 motion (*Hunt*, at para. 43) or to deny certification under s. 5(1)(a).

[181] Ontario cases have also suggested that an intrusion upon seclusion claim would be available for the type of information accessed in the present case, further demonstrating that the law on this issue is not settled.

[182] In *Broutzas*, Perell J. held that (i) the name and phone number information accessed for the purpose of selling RESPs to new parents was not sufficient to constitute an invasion of "private" information, and (ii) any such intrusion would not be "offensive" to a "reasonable person".

[183] However, Perell J. distinguished the facts of the case before him and those in *Tucci*. Perell J. stated that "the leaked information in the *Tucci* case exposed the Class members to identity theft and financial loss" (*Broutzas*, at para. 171).

[184] Consequently, the law is not settled that hacker access to information which can lead to identity theft cannot constitute an intrusion upon seclusion.

[185] Equifax relies on cases which hold that credit reports related to third party dealings are not subject to a claim for intrusion upon seclusion. Those cases rely on the principle that "credit checks do not give rise to [a legitimate privacy interest] because they tend to contain information about dealings with third parties" (see *Larizza v. The Royal Bank of Canada*, 2017 ONSC 6140 ("*Larizza*"), at para. 59).

[186] However, the financial and other personal information stored by Equifax was personal information of the Class members, not a credit report based on information from a "third party".

[187] Further, even the decisions relied upon by Equifax do not constitute settled law on the "credit report" issue. In *Jones*, Sharpe J.A. cited approvingly the decision of Stinson J. in *Somwar v. McDonald's Restaurants of Canada* (2006), 79 O.R. (3d) 172 (S.C.J.) ("*Somwar*"), in which the court dismissed a motion to strike the claim for invasion of privacy arising when the plaintiff's employer conducted a credit check on him without the plaintiff's consent (*Jones*, at

paras. 30-32). The court in *Somwar* appears to take a different approach than the court in *Larizza*.

[188] Finally, the comments of the court in *Kaplan-Certification*, relied upon by Equifax, cannot be taken as settled law that an intrusion upon seclusion claim cannot be brought against a Database Defendant for a hacker attack compromising information which could be used for identity theft.

[189] In *Kaplan-Certification*, the case was not certified because of a lack of commonality for the information disclosed (at para. 16). Only one of the five representative plaintiffs had a social insurance number and bank account information compromised. Belobaba J. held (at para. 64):

> The problem here is that the personal information that was stolen by the hacker and posted online consists of a disparate collection of unorganized documents and document fragments apparently taken from different types of folders. The type and amount of personal information posted online by the hacker varied widely from individual to individual.

[190] With respect to the nature of the information obtained, Belobaba J. commented (at para. 64) that "[s]ome of the personal information was private and confidential (banking details); much of it was relatively mundane (contact details only)". Belobaba J. later commented that there was no evidence to support an intrusion "in relation to private as opposed to simply personal information or that any such invasion or intrusion would be highly offensive to a reasonable person" (*Kaplan-Certification*, at para. 79).

[191] The decision in *Kaplan-Certification* does not stand for the principle that an action cannot be certified in which class members' social insurance numbers, e-mail addresses, dates of birth, names, and addresses[36] were hacked, exposing the class members to identity theft.

[192] In any event, the decision in *Kaplan-Certification* would not constitute "settled law" even if such a principle could be taken from the case, given the uncertainty in the law as discussed above and the decisions in *Broutzas* and *Tucci*.

3.3(f)(iv) Conclusion on the "significant invasion" requirement

[193] The issue of whether access to information which can lead to identity theft may be subject to an intrusion upon seclusion claim is not raised in *Jones*. Based on the reasons above, a court could find the disclosure of such information to be a "significant invasion of personal

[36] (and credit card information for 11,670 members of the group)

privacy" which is "offensive" to a "reasonable person".[37] Such an approach would be consistent with courts which have certified intrusion upon seclusion claims against Database Defendants when the information accessed could be used for identity theft.

[194] Consequently, it is not certain that the facts as pleaded cannot support this requirement for intrusion upon seclusion.

3.3(g) Conclusion on the Intrusion upon Seclusion Objection

[195] Based on the above case law, I find that it is not settled law that an intrusion upon seclusion claim is precluded against Equifax for the hacker attack. As a Database Defendant who allegedly recklessly allowed hackers to obtain social insurance numbers, credit card numbers, email addresses, names, addresses, and other information which collectively expose an individual to the risk of identity theft, it is not certain that the intrusion upon seclusion claim will fail.

[196] Consequently, I adopt the following submission of the plaintiff that Equifax's attempts to advocate for what the law should be are misplaced in a s. 5(1)(a) analysis when the law is not "settled" and "certain":

> While Equifax's arguments seeking to draw analogies based on various areas of law involve interesting questions of academic analysis, the issues are not appropriate to be determined at this stage of the proceeding. The fact that Equifax seeks to draw conclusions from a tapestry of different areas of the law, as opposed to decided cases under intrusion upon seclusion, is confirmation that the issues are not plain and obvious.

[197] Even if the liability of Database Defendants cannot be fully addressed by the reasons in *Jones*, whether intrusion upon seclusion can be extended based on the policy factors discussed in *Jones* should be determined at a hearing on the merits. As Wilson J. held in *Hunt* (at para. 48):

> While courts should pause before extending the tort beyond its existing confines, careful consideration might conceivably lead to the conclusion that the tort has a useful role to play in new contexts.

---

[37] In in a footnote to its factum, Equifax submitted that "even if the bald conclusions pled by the plaintiffs are found to technically satisfy the requirements of section 5(1)(a), which is denied, the plaintiffs have failed to establish some basis in fact for the allegation that the 'private affairs' of any putative class member have been invaded". That submission was not pursued at the hearing. In any event, given the uncontested evidence of the information accessed, I would find some basis in fact for the allegation that "private affairs" of a putative class member were invaded.

[198] For the above reasons, I find that the intrusion upon seclusion claim discloses a cause of action under s. 5(1)(a).

3.4 Objection 2: The Provincial Privacy Legislation Objection

[199] As with the Intrusion upon Seclusion Objection, Equifax submits that it is "plain and obvious" that the plaintiff cannot rely on the privacy legislation enacted in British Columbia, Saskatchewan, Manitoba, Newfoundland and Labrador, and Quebec. I do not agree.

3.4(a) The allegations in the Claim relevant to breach of provincial privacy legislation

[200] Owsianik relies on the same allegations as pleaded for the intrusion upon seclusion claim, with the additional allegations that:

(i) "[T]he actions of the defendants constitute wilful or intentional or reckless intrusions upon seclusion that would be highly offensive to a reasonable person";

(ii) "The defendants failed to take appropriate steps to guard against unauthorized access to sensitive financial information involving the Class Members'[38] private affairs or concerns"; and

(iii) "As a result, the defendants are liable under [the provincial privacy legislation]".

3.4(b) The applicable legislation

[201] In British Columbia, Saskatchewan, and Newfoundland and Labrador, each province has enacted a statute entitled the *Privacy Act*, which creates a statutory tort for a person who wilfully and without claim of right violates the privacy of another. By way of example, the *Privacy Act*, R.S.B.C. 1996, c. 373 provides (at s. 1(1)):[39]

> It is a tort, actionable without proof of damage, for a person, wilfully and without a claim of right, to violate the privacy of another.

[202] The Manitoba legislation creates a similar tort but does not require wilful conduct. Instead, the tort requires conduct which "substantially" and "unreasonably", without claim of

---

[38] As I discuss at paragraphs 22-24 above, the claim for breach of provincial privacy legislation is made only for the persons whose data was accessed (the Access-Only and Combined Subclasses).

[39] See also *Privacy Act*, R.S.S. 1978, c P-24, s. 2; *Privacy Act*, R.S.N.L 1990, c P-22, subs. 3(1).

right, violates the privacy of another person. Under s. 2(1) of *The Privacy Act*, C.C.S.M., c. P125:

> A person who substantially, unreasonably, and without claim of right, violates the privacy of another person, commits a tort against that other person.

[203] With respect to the claim under Quebec privacy legislation, the plaintiff relies on the *Civil Code of Quebec*, RLRQ, c. CCQ-1991 (the "*CCQ*"), art. 35-40.[40]

[204] Under section 37 of the *CCQ*, a person cannot "invade the privacy" of another. There is no requirement that the conduct be wilful or that it "substantially" and "unreasonably", without claim of right, violates the privacy of another person:

> 37. Every person who establishes a file on another person shall have a serious and legitimate reason for doing so. He may gather only information which is relevant to the stated objective of the file, and may not, without the consent of the person concerned or authorization by law, communicate such information to third persons or use it for purposes that are inconsistent with the purposes for which the file was established. *In addition, he may not, when establishing or using the file, otherwise invade the privacy or injure the reputation of the person concerned.* [Italics added.]

3.4(c) Overview of the parties' positions

[205] Equifax submits that it is plain and obvious that the breach of provincial privacy legislation claims must fail. Equifax submits that it is certain that:

(i) Its conduct cannot constitute a breach of the provincial privacy legislation because it was the hacker who "violated" or "invaded" the privacy" of another "without claim of right". This submission is similar to Equifax's position that no intrusion upon seclusion claim can be brought since Equifax did not access the information; and

(ii) Its conduct cannot constitute a breach of the provincial privacy legislation because the pleadings do not establish that it acted "wilfully", as required under the British Columbia, Saskatchewan, and Newfoundland and Labrador legislation. This submission is similar to Equifax's position that no intrusion upon seclusion claim can be brought since Equifax's conduct could not be found to be "reckless".

---

[40] In her initial factum, Owsianik also relied on *Act Respecting the Protection of Personal Information in the Private Sector*, L.R.Q., c. P-39.1, but advised the court prior to the hearing that she was not pursuing that claim.

[206] Owsianik submits that:

(i) It is not settled law that a Database Defendant who enables a hacker attack cannot be liable under the provincial privacy legislation. Owsianik relies on (a) cases which have certified claims under provincial privacy legislation against Database Defendants for hacker attacks and in other similar situations, and (b) general principles that the law concerning the statutory tort is broad, covers a wide spectrum of privacy interests, and is not fully defined by the courts; and

(ii) It is not settled law that "wilful" conduct cannot be established through the alleged conduct pleaded in the Claim. Owsianik relies on (a) cases which have certified breach of provincial privacy claims against Database Defendants for hacker attacks and in other similar situations and (b) the uncertainty in the law as to the meaning of "wilful" conduct.

[207] I address each issue below.

3.4(d) Issue 1: Is it settled law that the statutory tort is precluded for a hacker attack because it was the hackers who accessed the personal information?

[208] Equifax provided no case law that precludes the statutory tort against a Database Defendant for a hacker attack because the hackers, not the Database Defendant, accessed the personal information. Nor has Equifax provided any doctrinal support for its position. Again, while not necessarily determinative of a s. 5(1)(a) analysis, the lack of case law precluding such a claim is consistent with the uncertain state of the law.

[209] Equifax relies on the wording of the statutes, asking the court to find, on a s. 5(1)(a) analysis, that because the statutes require that the defendant either (i) "violates" the privacy of a person "without a claim of right" (as in the British Columbia, Saskatchewan, Manitoba, and Newfoundland and Labrador privacy legislation) or (b) "invade[s] the privacy" of a person (as in the Quebec legislation), a hacker attack cannot result in statutory liability against someone other than the hacker. However, the statutory language does not address whether a Database Defendant can invade a person's privacy by recklessly enabling a hacker attack.

[210] There is case law that has certified a statutory tort claim against Database Defendants who allegedly enabled hacker attacks or engaged in similar conduct.

[211] In *Hynes v. Western Regional Integrated Health Authority*, 2014 NLTD(G) 137, 357 Nfld. & P.E.I.R. 138 ("*Hynes*"), the plaintiffs alleged that the defendant hospital was responsible for an employee who had improperly accessed medical records. The hospital opposed certification of the statutory cause of action on the basis that nothing was pleaded to suggest that the hospital wilfully violated the plaintiffs' privacy. The plaintiffs sought certification of the action.

[212] Goodridge J. (as he then was) certified the action. With respect to the *Privacy Act* claim, he referred to the hospital's submissions, which were similar to those of Equifax discussed above (*Hynes*, at para. 18):

> The Defendant agrees that there would be a statutory cause of action against the employee, because she is the person who acted "wilfully and without a claim of right". *The Defendant disagrees that the pleadings establish a statutory cause of action against Western Health. It submits that (1) nothing is pleaded to suggest that the Defendant wilfully violated the Plaintiffs' privacy*; and (2) the common law doctrine of vicariously liable should not apply to this statutory tort. [Italics added.]

[213] Goodridge J. rejected those submissions. He held that the claim against the defendant that "it failed to establish safeguards" could be sufficient to establish that it "wilfully violated the Plaintiffs' privacy" under the *Privacy Act* (*Hynes*, at para. 19):

> *[T]he pleadings include a direct allegation against the Defendant, stating that it failed to establish safeguards. The determination of whether this alleged conduct is sufficient to establish that the Defendant "wilfully violated the Plaintiffs' privacy" will be determined at trial. It does not depend on vicarious liability*. Accordingly, I reject the Defendant's argument that nothing is pleaded to suggest that the Defendant wilfully violated the Plaintiffs' privacy. The alleged conduct of the employee may be a more obvious example of wilful conduct resulting in a violation of the Plaintiffs' privacy, but that too will need to be established at trial. [Italics added.]

[214] Equifax submits that *Hynes* is wrongfully decided. Equifax acknowledges that "the plaintiff in *Hynes* did assert a claim of direct liability under the *Privacy Act*" but submits that the approach of the court in *Hynes* "relieves the plaintiff of any obligation to plead material facts which, if proven, could potentially support the legal finding that the defendant acted wilfully or intentionally".

[215] Again, Equifax's submission that *Hynes* is not "good law" is not consistent with the *Hunt* test. The role of the court on a motion to strike or under s. 5(1)(a) is to determine whether there is settled law precluding the claim.

[216] In the recent decision of *Li c. Equifax Inc.*, 2019 QCCS 4340, [2019] J.Q. No. 8976 (C.S.) ("*Li*"),[41] Bisson J. held that the claim as pleaded supported a cause of action based on s. 37 of the *CCQ*, arising from the Data Breach. He held (at para. 23):

---

[41] The decision was released after submissions in the present motion but provided to the court by counsel.

> Le demandeur a également démontré une violation du droit à la vie privée, à la réputation et à la non-divulgation en communiquant ou en ne prévenant pas la communication à des tiers de renseignements confidentiels sans l'autorisation du demandeur.

[217] Consequently, the decision supports the availability of a statutory tort claim against Equifax for a hacker attack, subject to the issue of damages, which I address below.

[218] Bisson J. did not certify the claim in *Li*. Bisson J. relied on Quebec law that compensatory damages could not be claimed for a breach of s. 37 *CCQ* unless those damages had been incurred (*Li*, at paras. 24 and 28). In *Li*, the representative plaintiff only claimed compensatory damages (*Li*, at para. 25). As the representative plaintiff failed to establish any compensatory losses, certification was denied (*Li*, at paras. 27, 29-31, and 34).

[219] However, in the present case, Owsianik seeks "general damages to be assessed in the aggregate", consistent with the law in *Jones* that no actual damages are required under intrusion upon seclusion. Further, the plaintiff's position is consistent with the statutory tort, which is "actionable without proof of damage" under the British Columbia, Saskatchewan, and Newfoundland and Labrador legislation.

[220] Equifax provided no authority precluding a claim for general damages under the statutory tort. In contrast, the decisions in *Hynes* and *Bennett* are consistent with the position that it is not settled law that general damages are precluded under the statutory tort

[221] In *Bennett*, Belobaba J. certified the breach of provincial privacy claims, in which liability was claimed for exposing personal information to hackers. He held (*Bennett*, at para. 28):

> The scope and content of the provincial privacy laws in question is still evolving. In *Jones v. Tsige*, the Court of Appeal noted that 'no provincial legislation provides a precise definition of what constitutes an invasion of privacy.' It is therefore not plain and obvious that the secret installation of a 'malware' program 'designed [...] to invade the privacy of and cause harm to the class members' is not actionable as a privacy violation under the four provincial statutes.

[222] Equifax seeks to distinguish *Bennett* on the basis that Lenovo installed the malware that opened up potential access to hackers. However, as I discuss at paragraphs 126-28 above, it is not plain and obvious that the decision of the court in *Bennett* was limited to that basis.

[223] In *Bennett*, Belobaba J. relied upon an analogy of a landlord installing a peephole, which could result in a breach of statutory privacy laws even if no one used the peephole at a particular time (at para. 27). It is not certain that a similar analogy could not be applied to Equifax, who stored private information and allegedly recklessly permitted others to "peep" into the class members' personal financial information.

[224] Further, courts have cautioned against limiting the scope of breach of provincial privacy legislation claims on a pleadings motion, since the law in this area is only recently developing.

[225] In *Bigstone v. St. Pierre*, 2011 SKCA 34, 371 Sask. R. 35 ("*Bigstone*"), the plaintiff alleged intentional conduct by the hospital employee in accessing the plaintiff's records, and vicarious liability for the hospital. Ottenbreit J.A. held that it was inappropriate to strike the claim under *The Privacy Act*, R.S.S. 1978, c. P-24 (the "Saskatchewan *Privacy Act*").

[226] *Bigstone* did not address whether a Database Defendant can be liable under provincial privacy legislation for allowing a hacker to access personal information. However, Ottenbreit J.A. held that (i) the concept of privacy under the Saskatchewan *Privacy Act* is "arguably quite broad" (at para. 23); (ii) it can "cover a wide spectrum of privacy interests" (at para. 26); and (iii) "the essential elements of the statutory tort have yet to be fully defined by our courts" (at para. 19).

[227] Ottenbreit J.A. held that if the claim alleges (i) the action is pursuant to the Saskatchewan *Privacy Act*; (ii) the impugned conduct falls within the arguable scope of the Saskatchewan *Privacy Act*; (iii) the privacy is that of a person; (iv) the type of privacy interest is generally identifiable; and (v) the violation is wilful and without claim of right, a claim under privacy legislation could stand "[a]t this stage of the development of the jurisprudence respecting the *Act*" (*Bigstone*, at para. 34).

[228] Based on the above law, I find that a claim for breach of provincial privacy legislation against Equifax arising from a hacker attack is not certain to fail. The courts have not addressed the merits of the issue, and those courts which have considered similar situations have certified claims on this basis. Even if the issue is novel and cannot be addressed by the existing case law, it should not be decided on a certification motion, where settled law is required.

3.4(e) Issue 2: Is it plain and obvious that the conduct of Equifax cannot be found to be "wilful"?[42]

[229] These submissions by Equifax track, to a large extent, its submissions that the pleadings do not support a finding that it could be reckless, as required under the case law for intrusion upon seclusion.

[230] As I discuss at paragraphs 213 and 221 above, the decisions in *Hynes* and *Bennett* found a cause of action to exist under the provincial privacy statutes, since it was not certain that "wilful" conduct could not be established on the allegations in the pleadings.

---

[42] (This requirement is found only in the B.C., Saskatchewan, and Newfoundland and Labrador statutes.)

[231] In the present case, the plaintiff alleges that Equifax (i) knew from three leading outside consultants that its IT system was grossly deficient and left sensitive customer information vulnerable to hackers, (ii) knew that the Apache Struts vulnerability left the information open to hacker attack in a "highly dangerous and especially easy to exploit" manner, and (iii) yet still failed to patch systems in a timely or proper manner with the information stored in unencrypted form. It is not plain and obvious that a court could not find that Equifax wilfully ignored the risks of a hacker attack, which could then be considered under the provincial privacy statutes.

[232] Equifax relies on the decision of the B.C. Court of Appeal in *Duncan v. Lessing*, 2018 BCCA 9, 5 B.C.L.R. (6th) 81 ("*Duncan*"), in which the court considered whether disclosure by counsel of a party's private information in application materials prepared in the course of judicial proceedings gives rise to a cause of action under the *Privacy Act* (*Duncan*, at para. 3).

[233] However, the court in *Duncan* did not establish a definition of wilful conduct. Instead, it commented that an earlier decision of the British Columbia Court of Appeal in *Hollinsworth v. BCTV, a division of Westcom TV. Group Ltd.*, (1998), 59 B.C.L.R. (3d) 121 ("*Hollinsworth*"), which had also considered the meaning of the word "wilful" in the context of the privacy legislation, might need to be reconsidered. This does not create settled law that Equifax's conduct cannot be found to be wilful.

[234] In *Hollinsworth*, the court imported an objective element into the "wilful" requirement by finding that "wilful" conduct could arise upon "an intention to do an act which the person doing the act knew or should have known would violate the privacy of another person" (*Duncan*, at paras. 29-30).

[235] In *Duncan*, the court questioned, without deciding, whether the objective test in *Hollinsworth* was correct. Hunter J.A. commented that "the inclusion of the objective standard 'should have known' [in *Hollinsworth*] may not capture the deliberateness that is implicit in the word 'wilfully'" (*Duncan*, at para. 84).

[236] Hunter J.A. noted that "[t]he term "wilfully" appears in many statutes and is "usually defined as meaning deliberately, intentionally or purposefully" (*Duncan*, at para. 86). The court concluded that while "[i]t is not necessary for the purposes of this appeal to define with precision the definition of the term […] it can be said with some confidence that 'wilfully' does not mean accidentally" (*Duncan*, at para. 86).

[237] Consequently, the law is uncertain as to whether an objective aspect can be applied to the statutory requirement of "wilful" conduct. The decision in *Duncan* does not yield a settled result as to the scope of "wilful" conduct, and on that basis (as well as the law set out in *Hynes* and *Bennett*), I reject Equifax's submission that it is plain and obvious that it cannot be found to have engaged in wilful conduct.

[238] Even if "wilful" conduct requires "deliberate" behaviour, there is no case law before the court to determine whether such conduct includes recklessness, as was adopted by the court in

Jones in relation to intrusion upon seclusion. The scope of "wilful" conduct under the statutory tort is not settled.

[239] Further, given that Owsianik pleads deliberate and intentional conduct, a test of "non-accidental" conduct as suggested in *Duncan* could still be met.

[240] I again rely on the decision in *Bigstone* which sets out the broad scope of a breach of provincial privacy legislation claim at the pleadings stage in order to ensure "the development of the jurisprudence respecting the *Act*" (*Bigstone*, at para. 34).

3.4(f) Conclusion on the Provincial Privacy Legislation Objection

[241] There is case law in which courts have found a cause of action was disclosed under provincial privacy statutes against Database Defendants arising from a hacker attack. The decision in *Bennett* is consistent with that result. Further, the definition of "wilful" conduct has not been settled. Under the *Hunt* test, it is not appropriate to prevent the law from developing as to the "wilful" requirement under the provincial privacy legislation.

[242] For the above reasons, I do not find that it is certain that the plaintiff cannot succeed under the provincial privacy legislation in British Columbia, Saskatchewan, Manitoba, Quebec, and Newfoundland and Labrador.

3.5 Objection 3: The Breach of Contract Objection

[243] Equifax submits that it is certain that there is no cause of action for breach of contract for those subscribers whose data was not accessed (the Contract-Only Subclass).

[244] Equifax submits that the contractual claim of the subscribers is limited to "expectation" (compensatory) loss. Equifax submits that the subscribers in the Contract-Only Subclass suffered no such loss since they were in the same position as if the contract had not been breached, *i.e.* their personal information was not accessed. Consequently, Equifax submits that the Contract-Only subscribers have no cause of action.

[245] The corollary of Equifax's position is that while members of the Combined Subclass have a contractual claim, they can only seek expectation damages, and must establish those damages on an individual basis.

[246] Owsianik submits that it is not settled law that subscribers are limited to expectation damages for breach of contract. Owsianik submits that the subscribers paid for services they did not receive, and as such are entitled to restoration of the benefits conferred on Equifax, as damages for the alleged breach of contract. Owsianik pleads that "[t]he defendants are liable to repay all fees paid by Class Members".

[247] The corollary of Owsianik's position is that it is not settled law that individual trials would be required for the Combined Subclass since restitutionary or nominal damages may be available and could be determined without individual assessment.

[248] Further, Owsianik submits that Equifax's breach of the contract could result in an award of nominal damages which can also support certification of a breach of contract claim.

[249] Consequently, Owsianik submits that it is not plain and obvious that (i) the claim for "restitutionary"[43] damages to restore the benefits conferred to Equifax is not available to subscribers or (ii) certification cannot be granted for a nominal damages claim.

3.5(a) The allegations in the Claim relevant to breach of contract

[250] I have set out the allegations relevant to the breach of contract claim at paragraphs 55 to 57 above.

[251] In brief, Owsianik pleads that Equifax was contractually required to be a "trusted steward of personal information", "committed to protecting the personal information under our control", using "strict security safeguards" by agreeing to "regularly review, test and enhance our systems to ensure they meet accepted industry standards".

[252] Owsianik pleads that Equifax breached those contractual obligations to its subscribers since Equifax (i) knew from three leading outside consultants that its IT system was grossly deficient and left sensitive customer information vulnerable to hackers, (ii) knew that the Apache Struts vulnerability left the information open to hacker attack in a "highly dangerous and especially easy to exploit" manner, and (iii) yet still failed to patch systems in a timely or proper manner with the information stored in unencrypted form.

3.5(b) A preliminary issue: Should the breach of contract and consumer protection claims of the Contract-Only Subclass raised under s. 5(1)(a) be addressed on this certification motion?

[253] Owsianik submits that the court should not consider whether the breach of contract or consumer protection claims of the Contract-Only Subclass disclose a cause of action, since Equifax acknowledges that the breach of contract claim (on which PCIs (xi)-(xiv) arise) and the

[43] I use the term "restitutionary" to distinguish between "compensatory" or "expectation" damages intended to place a plaintiff in the position the plaintiff would have been if the contract had not been breached. However, as I discuss below, there is a distinction between restitutionary damages based on the disgorgement of profit (which is not sought by the plaintiff) and restitutionary damages to restore benefits for contractual services which were not received (which is sought by the plaintiff).

consumer protection claim (on which PCIs (xv) – (xvii) arise)[44] can proceed on a common basis for the subscribers whose data was accessed (the Combined Subclass). The plaintiff relies on the following principles:

(i) "[E]ven a significant level of differences among the class members does not preclude a finding of commonality." If "material differences emerge, the court can deal with them when the time comes" (*Pro-Sys*, at para. 112);

(ii) "[A] question will be considered common if it can serve to advance the resolution of every class member's claim. As a result, the common question may require nuanced and varied answers based on the situations of individual members" (*Vivendi Canada Inc. v. Dell'Aniello*, 2014 SCC 1 ("*Vivendi*"), at para. 46);

(iii) The commonality requirement does not mean that an identical answer is necessary for all members of the class, or even that the answer must benefit each of them to the same extent (*Vivendi*, at para. 46); and

(iv) It is enough that the answer to the question does not give rise to conflicting interests among the members (*Vivendi*, at para. 46).

[254] On the basis of the above principles, Owsianik submits:

> [T]here is no reason for which the breach of contract[45] common issues cannot be decided for everyone, leaving the Court to determine liability and damages based on different categories of claims: persons who can prove breach of contract, and persons who cannot; persons who can prove harm, and persons who cannot […];
>
> [T]here is no valid reason to ask this Court to decide that it is plain and obvious that persons who suffered no actual loss are not entitled to be members of the class because they have no valid claim at law. Equifax can seek to move to decide these issues summarily after certification, if appropriate, but there is no valid purpose to decide these issues prior to certification. It will not affect the class definition or the certified common issues relating to breach of contract.

[255] While the general principles relied upon by the plaintiff are not in dispute, I do not find that they should be applied when the claim of an entire subclass is contested under s. 5(1)(a). Equifax submits that the approximately 300,000 members of the Contract-Only Subclass cannot

[44] (except for the rescission or damages remedy claimed by the Combined Subclass under PCI (xviii), for which Equifax asserts no common issue arises, an issue I address below)

[45] The plaintiff makes similar submissions for the consumer protection claims of the Contract-Only Subclass.

bring any claim, since the breach of contract and breach of consumer protection legislation claims upon which they rely allegedly disclose no cause of action. If the only claims relied upon by those subclass members are certain to fail, then there is no "answer" to obtain at trial for them.

[256] Consequently, I do not accept the plaintiff's preliminary objection that the s. 5(1)(a) analysis for the breach of contract and consumer protection claims should be discarded for the Contract-Only Subclass because "[i]t may be that some class members can prove a breach of contract and/or damages, while others cannot". If there is no cause of action under s. 5(1)(a) for the Contract-Only Subclass, the claim should not be certified for them.

3.5(c) Overview of the parties' positions

3.5(c)(i) The position of Equifax

[257] Equifax acknowledges that the PCIs for the breach of contract claims can be certified with respect to the Combined Subclass.[46] Those PCIs are:

> PCI (xi): For Class Members that purchased Equifax Complete Advantage, Equifax Complete Premier, Equifax Complete Friends and Family or any other Equifax product offering credit monitoring and identity theft protection, was it a term of the contract that the defendants would maintain strict security safeguards when storing personal information?
>
> PCI (xii): Did the defendants comply with the contract by failing to apply a security patch made available in March 2017 until August 2017?
>
> PCI (xiii): For Class Members that purchased Equifax Complete Advantage, Equifax Complete Premier, Equifax Complete Friends and Family or any other Equifax product offering credit monitoring and identity theft protection, was it a term of the contract that the defendants would provide information to Members to help them minimize the risk of identity theft and to prepare them to respond to a real and/or suspected act of identity theft?
>
> PCI (xiv): Did the defendants comply with the contract?

[258] However, Equifax submits that those PCIs cannot be certified for the Contract-Only Subclass (*i.e.* those class members who held subscription contracts with Equifax but whose data

[46] Subject to Equifax's position that the damages sought by the Combined Subclass in contract must be determined on an individual basis, given Equifax's position that it is plain and obvious that (i) restitutionary damages are not available to any subscriber and (ii) a nominal damages claim cannot be certified.

was not accessed by hackers). Equifax submits that the Contract-Only Subclass suffered no expectation damages and, therefore, cannot maintain a claim in contract.

[259] In brief, Equifax submits that it is plain and obvious that (i) the pleadings cannot support a claim for restitutionary damages for any subscriber[47] and (ii) a contract claim based solely on nominal damages ought not be certified.

[260] Equifax relies on cases in which restitution based on disgorgement of profit was sought. Equifax submits that such restitution is exceptional relief and can only be granted for breach of contract in situations akin to a breach of trust or breach of fiduciary duty. Equifax submits that it is plain and obvious that such circumstances do not arise in the present case.

[261] Equifax also relies on a series of data breach class action cases in which only customers of the bank or patients at a hospital whose data was accessed brought claims in contract as class members (*Evans v. Bank of Nova Scotia*, 2014 ONSC 2135 ("*Evans*"), at paras. 35-36 and 69; *Hynes*, at paras. 39-45 and 53; *Daniells v. McLellan*, 2017 ONSC 3466 ("*Daniells*"), at paras. 23, 27 and 114-15; and *Condon v. Canada*, 2014 FC 250 ("*Condon*"), at para. 47, appeal allowed on certification of negligence and breach of confidence claims, 2015 FCA 159).

[262] Equifax relies on the above cases to submit that permitting the Contract-Only Subclass to bring an action for restitutionary or nominal damages would "open the floodgates" to litigation by bank customers or hospital patients whose data is not accessed.

[263] Finally, Equifax submits that restitution is not available because Equifax provided many of the services for which it contracted.

3.5(c)(ii) The position of the plaintiff

[264] Owsianik submits that it is not plain and obvious that (i) restitutionary damages cannot be awarded to restore benefits paid for services not provided or (ii) a contract claim based solely on nominal damages cannot be certified.

[265] With respect to the restitution claim, the plaintiff submits that the facts as pleaded could support a finding by the common issues judge that restitutionary damages be awarded because the subscribers paid for data protection which was not provided (in whole or in part).

[266] Even under the disgorgement case law relied upon by Equifax, the plaintiff submits[48] that it is not settled law that restitutionary damages are not available. Under that case law, the

[47] A "subscriber" includes any person in Canada who subscribed to the Subscription Products between March 7, 2017 and July 30, 2017, whether in the Contract-Only or Combined Subclasses.

plaintiff submits that it is not certain that the ordinary damages remedy for the underlying wrong is adequate, particularly given (i) the position Equifax took as a "trusted steward" of its subscribers' personal information and (ii) the need for deterrence.

[267] Finally, Owsianik submits that the law is not settled that certification must be denied for a nominal damages claim.

[268] For the reasons that follow, I agree with the position of Owsianik. I address the restitutionary and nominal damages issues below.

3.5(d) The claim for restitutionary damages

3.5(d)(i) The applicable law

[269] It is settled law that a plaintiff who suffers a breach of contract will generally be entitled only to expectation damages. In *Bank of America Canada v. Mutual Trust Co*., 2002 SCC 43, [2002] 2 S.C.R. 601 ("*BOA*"), the court held (at paras. 26-27):

> Generally, courts employ expectation damages where, if breach is proved, the plaintiff will be entitled to the value of the promised performance. […]
>
> […] The rule of the common law is, that where a party sustains a loss by reason of a breach of contract, he is, so far as money can do it, to be placed in the same situation, with respect to damages, as if the contract had been performed.

[270] Equifax relies on cases in which disgorgement of profits was sought. In *Apotex Inc. v. Eli Lilly and Company*, 2015 ONCA 305, 125 O.R. (3d) 561 ("*Apotex*"), Apotex sought disgorgement of profits from a defendant pharmaceutical manufacturer arising from an invalidated patent. The court relied on the principle that disgorgement of profits is available only in exceptional circumstances, when "the ordinary damages remedy for the underlying wrong is inadequate", and dismissed Apotex's appeal. Feldman J.A. held (at para. 47):

> Apotex also points to some cases where a remedial claim for disgorgement of profits has been awarded despite the absence of any quantifiable loss to the plaintiff. *These cases arise where a defendant has committed an underlying legal wrong against a plaintiff, and the ordinary damages remedy for the underlying wrong is inadequate. The 'wrong' in these contexts typically consists of a breach*

---

[48] In her factum, the plaintiff does not make this submission as an alternative argument, but instead responds to the disgorgement of profit cases relied upon by Equifax. However, as set out in the Claim and as submitted at the hearing, Owsianik pleads that "[t]he defendants are liable to repay all fees paid by Class Members." Consequently, I review the response to the disgorgement of profit cases as an alternative submission.

> *of fiduciary duty or a breach of trust, and in some instances has involved criminal conduct, breach of contract or a tort committed against the plaintiff. Courts that have applied this restitutionary remedy in non-fiduciary contexts have explained that it is limited to exceptional cases, emphasizing that restitution damages are employed infrequently*: see, e.g., *Bank of America Canada v. Mutual Trust Co*., 2002 SCC 43 (CanLII), [2002] S.C.R. 601, at para. 25, referred to by Winkler C.J.O. in *Cassano v. Toronto Dominion Bank*, 2007 ONCA 781 (CanLII), 87 O.R. (3d) 401, at para. 27. [Italics added.]

[271] In *Apotex*, the court referred to the House of Lords decision in *Attorney General v. Blake*, 2000 UKHL 45 ("*Blake*"), in which disgorgement of profit was sought from a former member of the Secret Intelligence Service of Great Britain, who wrote a book disclosing state secrets and was then sued by the Attorney General for breach of contract. The court relied on *Blake* for the governing principle that restitutionary relief seeking disgorgement of profits is "exceptional", arising "where the normal remedies were inadequate and where deterrence of others was an important factor" (*Apotex*, at paras. 48-49):

> [I]n *Attorney General v. Blake*, [2000] UKHL 45, [2001] 1 A.C. 268, a former member of the Secret Intelligence Service ('SIS') of Great Britain disclosed valuable secrets to the Soviet Union. He was convicted of spying, and ultimately defected to the U.S.S.R. As an employee of the SIS, he had signed an undertaking not to divulge any official information that he acquired in the course of his employment. While living in the Soviet Union, he wrote a book disclosing former state secrets – although by then, much of the information was no longer secret. The Attorney General sued Blake for breach of contract and sought disgorgement of his profits.
>
> The House of Lords ordered an accounting of profits. *The court referred to this as an 'exceptional' case of breach of contract, akin to a breach of fiduciary duty, where the normal remedies were inadequate and where deterrence of others was an important factor, thereby justifying the imposition in this case of the remedy of a full accounting of profit.* [Italics added.]

[272] The basis for restricting the disgorgement of profits to exceptional circumstances is reviewed by Iacobucci J. in *BOA*, at paras. 30-31:

> The other side of the coin is to examine the effect of the breach on the defendant. In contract, restitution damages can be invoked when a defendant has, as a result of his or her own breach, profited in excess of his or her expected profit had the contract been performed but the plaintiff's loss is less than the defendant's gain. So the plaintiff can be fully paid his damages with a surplus left in the hands of the defendant. This occurs with what has been described as an efficient breach of contract. In some but not all cases, the defendant may be required to pay such profits to the plaintiff as restitution damages (Waddams, supra, at p. 474).

> Courts generally avoid this measure of damages so as not to discourage efficient breach (i.e., where the plaintiff is fully compensated and the defendant is better off than if he or she had performed the contract) (Waddams, *supra*, at p. 473). Efficient breach is what economists describe as a Pareto optimal outcome where one party may be better off but no one is worse off, or expressed differently, nobody loses. Efficient breach should not be discouraged by the courts. […]

[273] Consequently, it is settled law that the disgorgement of profits as a restitutionary remedy is exceptional relief.

[274] However, Owsianik does not make a "profit disgorgement" claim. Instead, the subscribers seek the return of funds paid for services not rendered, which are "restitutionary" in that the defendant must return those benefits, but not "profits" from an "efficient breach".

[275] It is not settled law that the restitutionary damages sought by the subscribers violates the expectation damages principle. Owsianik's position is that the relief sought by the subscribers would not discourage efficient breach. Rather, allowing Equifax to retain the benefits without providing services would result in a "zero-sum" outcome, rather than a Pareto optimal outcome, with Equifax receiving the benefits of payment and the subscriber being "worse off" because he or she paid for services and received no benefit.

[276] The above distinction was noted in *BOA*. The court held that "[t]his is not a case of efficient breach", since the compound interest was the subject of the agreement between the parties and "[a]n award of compound interest will prevent the respondent from profiting by its breach at the expense of the appellant" (at para. 61).

[277] Professor Waddams also addresses this distinction, in *The Law of Damages*, Looseleaf Edition (Canada Law Book: November 2018) ("Waddams"). He first reviews the restitution of profits case law from *BOA* and *Blake* and concludes (at para. 9.200) (footnotes omitted):

> No general principle exists whereby a defendant can be made to account for a profit derived from a simple breach of contract. Unless the plaintiff is entitled to specific performance, the defendant is allowed to break the contract on payment of compensation. Economists have argued that breach in these circumstances is efficient, because the defendant gains by the breach and the plaintiff, being fully compensated, is no worse off.

[278] Professor Waddams then distinguishes the "profit disgorgement" cases from those in which restitutionary damages may be awarded for moneys paid for services not rendered (at para. 9.220):

> Although, as it has been said, there is no general principle requiring the defendant to account for profits derived from a breach of contract, the defendant can, in some circumstances, be required to restore the benefits conferred by the plaintiff.

[279] Professor Waddams summarizes the state of the law on the availability of restitutionary damages to restore benefits conferred to a defendant who does not perform all (or part) of the contractual services (at paras. 9.220 and 9.230) (footnotes omitted):

> (i) The "typical case is where the plaintiff pays in advance for a performance that the defendant wholly fails to render. The plaintiff is entitled to recover the money. […] *Though older cases had denied a remedy unless the contractual performance by the defendant had wholly failed, more recent cases suggest that receipt of some benefit by the plaintiff is not always a bar"*;
>
> (ii) "Receipt of a substantial benefit, however, will often raise problems of valuation and where the plaintiff has an adequate remedy for breach of contract, the difficulty of valuing benefits received will justify the court in restricting the plaintiff to the contractual remedy"; and
>
> (iii) *The "basis for the plaintiff's claim in such cases is restitutionary. The plaintiff claims not compensation for breach of the contract but restitution of the benefits conferred, because it is unjust that the defendant should retain them*." [Italics added.]

3.5(d)(ii) Analysis

[280] Based on the above law, I find that it is not plain and obvious that a subscriber could not obtain restitutionary damages to return fees paid to Equifax between March 7, 2017 and July 30, 2017.

[281] Based on the pleadings, Equifax collected monthly subscription fees for (i) acting as a "trusted steward" of personal information, (ii) being "committed to protecting the personal information under our control", (iii) "maintain[ing] strict security safeguards when storing or destroying your personal information in order to prevent unauthorized access, collection, use, disclosure […] or similar risks", and (iv) "regularly review[ing], test[ing] and enhanc[ing] our systems to ensure they meet accepted industry standards".

[282] Based on the pleadings, Equifax collected monthly subscription fees from its subscribers under "grossly deficient" security, using outdated and obsolete software.

[283] Counsel at the hearing advised that monthly subscription fees were approximately $20. With over 300,000 Contract-Only Subclass members,[49] and additional subscribers from the

[49] (see footnote 9 for details on the calculation)

Combined Subclass, Equifax would have received more than $6 million per month from its Canadian subscribers while allegedly failing to provide data protection.

[284] In essence, the subscribers submit that they paid monthly fees for data protection services which were not provided. In the Claim, the allegations support (i) grossly inadequate and dangerously deficient cybersecurity, (ii) data protection measures which failed to meet the most basic industry standards, (iii) a failure to encrypt data, (iv) outdated and obsolete software, and (v) Equifax's failure to heed advice by external security experts warning of inadequacies in cybersecurity.

[285] Even if Equifax rendered part of its services, restitutionary damages could be available, following the principles summarized by Professor Waddams that any "problems of valuation" can be determined if "the plaintiff [does not have] an adequate remedy for breach of contract".

[286] Consequently, it is not settled law that restitutionary damages to return fees paid are not available.

[287] For the same reasons, it is not settled law that restitution is not available to the Combined Subclass subscribers, regardless of whether they also suffered compensatory losses.

[288] I also note that, even if the "disgorgement of profit" cases relied upon by Equifax applied to the subscribers' contractual claims, it would not be settled law that a restitutionary claim was not available. Under *Apotex*, a court could order restitution when "the ordinary damages remedy for the underlying wrong is inadequate". In the present case, as the Contract-Only subscribers allegedly paid for services they did not receive (in whole or in part), a court could find that "deterrence" is an important factor, and order that amounts paid for services rendered be returned.

[289] Even if (i) the *Apotex* approach applied and (ii) the court required a "trust-like" relationship to order restitutionary damages,[50] a court could find that the nature of the contractual relationship was akin to a trust in that Equifax represented itself to be a "trusted steward" paid monthly to store, and protect against identity theft, personal and sensitive financial information of its subscribers. Equifax promised to maintain "strict security safeguards" when storing "all information", by exercising "high standards". It is not plain and obvious that Equifax does not have a "trust-like" role as guardian of a subscriber's sensitive personal information.

---

[50] Based on *Apotex*, it is not settled law that a trust-like or fiduciary-like relationship is required for disgorgement of profit, given the comments of the court that restitution can be ordered "where a defendant has committed an underlying legal wrong against a plaintiff, and the ordinary damages remedy for the underlying wrong is inadequate", with the wrong including a "breach of contract". The court only noted that trust-like cases are "typically" when restitution is ordered – see *Apotex*, at para. 47.

[290] Further, I do not accept the "floodgates" argument of Equifax that permitting the present claim to proceed for the Contract-Only Subclass will lead to claims by "hundreds of thousands" or "millions" (as submitted by Equifax) of bank customers or hospital patients upon a data breach.

[291] It would be improper for the court to speculate on facts not before it. Future courts can consider whether a claim against a company who charges clients a monthly subscription fee to protect subscribers against identity theft and then fails to provide some or all of those services (as alleged in the present case) can be distinguished from claims against institutions such as banks and hospitals, which hold confidential information about their clients because they are required to do so, but are not in the business of charging fees to store and protect that information.

[292] In the latter circumstances (which arise in the decisions of *Evans*, *Daniells*, *Hynes*, and *Condon* relied upon by Equifax), restitution may not be available because no fees were paid which ought to be restored. In these circumstances, claims may be limited to those persons whose data was accessed, as opposed to all customers of the bank or patients in a hospital. In the cases relied upon by Equifax, no claim was made by persons whose data was stored but not accessed.

[293] Consequently, I find that if the common issues judge concludes there was a breach of contract because Equifax failed to maintain strict security standards, it is not plain and obvious that the subscribers would be precluded from obtaining restitution of fees paid (in whole or in part) between March 7, 2017 and July 30, 2017.

3.5(e) The nominal damages claim

[294] Given my conclusion that the pleadings disclose a cause of action for restitutionary damages for subscribers, it is not necessary to determine whether the claim could be certified only for nominal damages.

[295] However, I briefly address Equifax's position that it is settled law that a claim only for nominal damages cannot be certified.

[296] Nominal damages can be awarded if the plaintiff establishes a breach of contract but fails to establish a loss caused by the wrong (Waddams, at para. 10.10).

[297] Equifax relies on the recent costs endorsement of Belobaba J. in *Kaplan v. Casino Rama Services Inc.*, 2019 ONSC 3310 ("*Kaplan–Costs*"), in which he commented that (i) the only "tenuous" breach of contract claim was for nominal damages, and (ii) he would not have certified the claim on that basis (*Kaplan-Costs*, at para. 5) (footnotes omitted):

> A nominal damages award (of say $1 per claimant, resulting in a total award of about $10,000) would not have justified this proposed class action on any of the traditional rationales – access to justice, judicial economy or behaviour modification.

[298] In *Kaplan-Costs*, it appears that no restitutionary damages were sought by the plaintiff, in circumstances in which the information was held by the defendant casino but was not the subject of monthly subscription fees being paid to protect the information.[51]

[299] I note that nominal damages may be more than the $1 per claimant used as an example in *Kaplan-Costs*. In *Heckert v. 5470 Investments Ltd.*, 2008 BCSC 1298, 299 D.L.R. (4th) 689 ("*Heckert*"), a privacy case cited by Sharpe J.A. in *Jones*, nominal damages of $3,500 were awarded (*Heckert*, at para. 151). With over 300,000 Contract-Only subscribers, and additional subscribers from the Combined Subclass, the factors relied upon by Belobaba J. in *Kaplan-Costs* might not arise on the facts of the present case.

[300] Consequently, it is not settled law that a claim for nominal damages cannot be certified.

3.5(f) Conclusion on the Breach of Contract Objection

[301] For the above reasons, I do not find it certain that the breach of contract claim by the Contract-Only Subclass would fail. I find that the claim discloses a cause of action for restitutionary and nominal damages.

[302] For the same reasons, I also find that it is not plain and obvious that the contractual claim of the Combined Subclass would be limited to expectation damages.

3.6 Objections 4 and 5: The Consumer Protection Legislation Objections

3.6(a) The positions of the parties

[303] Both the Consumer Protection Cause of Action Objection and the Consumer Protection Common Issue Objection (collectively, the "Consumer Protection Legislation Objections") are based on s. 18 of the *Consumer Protection Act* ("s. 18").

[304] As with the issue of breach of contract, Equifax acknowledges that the Combined Subclass has pleaded a cause of action for breach of consumer protection legislation which engages the following PCIs:

> PCI (xv): Did the defendants (or any of them) make false, misleading or deceptive representations within the meaning of the *Consumer Protection Act, 2002* or the Equivalent Consumer Protection Statutes (as defined in the Statement of Claim)?

[51] (circumstances similar to the other cases relied upon by Equifax as I discuss at paragraph 292 above)

PCI (xvi): If so, were any such representations unconscionable?

PCI (xvii): Is it in the interests of justice to disregard the requirement to give notice under the *Consumer Protection Act, 2002* or the Equivalent Consumer Protection Statutes (as defined in the Statement of Claim)?

[305] However, Equifax opposes certification of PCI (xviii) which provides:

> Are the class members, or any of them, entitled to rescission or damages under the *Consumer Protection Act, 2002* or the Equivalent Consumer Protection Statutes (as defined in the Statement of Claim)?

[306] With respect to the Consumer Protection Cause of Action Objection, Equifax submits that no cause of action arises for the Contract-Only Subclass because it is settled law that (i) those subscribers have suffered no compensable damages and, as such, cannot obtain damages under s. 18 and (ii) rescission is not available under s. 18 since the contract services were provided.

[307] With respect to the Consumer Protection Common Issue Objection, Equifax submits that the Combined Subclass cannot certify their consumer protection claims under s. 18 as a common issue since (i) those subscribers can only claim for compensable damages under s. 18, which raise individual issues and (ii) rescission is not available under s. 18 because the contract services were provided.

[308] For both objections, Owsianik submits that it is not settled law that the subscribers cannot claim (i) restitutionary and nominal damages under s. 18 or (ii) rescission under s. 18 by all current subscribers,[52] as a result of Equifax's alleged unfair practices in its representations to its subscribers.

3.6(b) The allegations in the Claim relevant to breach of consumer protection legislation

[309] I have set out the allegations relevant to the breach of consumer protection legislation claim at paragraph 71 above.

[310] Owsianik pleads that Equifax engaged in "unfair practices" under the *Consumer Protection Act* by making false, misleading or deceptive representations, including that it (i)

[52] Owsianik acknowledges that to the extent rescission is available, it can only be sought by those subscribers who currently remain an Equifax subscriber.

maintains strict security safeguards when storing personal information, (ii) is "committed to protecting the personal information under our control", and (iii) takes steps to "regularly review, test and enhance our systems to ensure they meet accepted industry standards".

3.6(c) Section 18

[311] Section 18 provides:

> Rescinding agreement
>
> 18 (1) Any agreement, whether written, oral or implied, entered into by a consumer after or while a person has engaged in an unfair practice may be rescinded by the consumer and the consumer is entitled to any remedy that is available in law, including damages. 2002, c. 30, Sched. A, s. 18(1).
>
> Remedy if rescission not possible
>
> (2) A consumer is entitled to recover the amount by which the consumer's payment under the agreement exceeds the value that the goods or services have to the consumer or to recover damages, or both, if rescission of the agreement under subsection (1) is not possible,
>
> (a) because the return or restitution of the goods or services is no longer possible; or
>
> (b) because rescission would deprive a third party of a right in the subject-matter of the agreement that the third party has acquired in good faith and for value. 2002, c. 30, Sched. A, s. 18 (2); 2004, c. 19, s. 7 (6).

3.6(d) The applicable law

[312] The court in *Ramdath v. George Brown College of Applied Arts and Technology*, 2015 ONCA 921, 341 O.A.C. 338 ("*Ramdath CA*") held that that all common law damages are available under s. 18(2). Feldman J.A. stated (at para. 94):

> In my view, it was open to the trial judge to accept the parties' agreement to use the tort measure of damage, and also to apply their agreed formula. In his text, *The Law of Damages*, referred to by the trial judge, Professor Waddams discusses the measure of damages in statutory remedies for misrepresentation, including the Ontario *Consumer Protection Act*. He explains *that the language of s. 18(2) that prescribes the compensation entitlement for a plaintiff, together with the availability of punitive and exemplary damages in s. 18(11), give a court 'complete flexibility to award whatever damages would be appropriate at common law' including the restitutionary measure.* Having said that, he would reject using the contractual measure: see Steven M. Waddams, *The Law of*

> *Damages*, loose-leaf, 2nd ed. (Toronto: Canada Law Book, November 2015 release at paras. 5.690 to 5.700). [Italics added.]

[313] It is not necessary to establish that damages were sustained as a result of the alleged unfair practice. In *Ramdath CA*, the court held (at para. 90):

> [T]he necessary causal link [to claim and recover damages] is the link between the damages and the agreement, i.e. that the consumer suffered damages that flowed from entering into an agreement after or while an unfair practice was occurring. What is not required is a causal link between the actual unfair practice and the damages. That is because damages are payable regardless of reliance. To require the causal link suggested by [the defendant] would reintroduce the need for reliance or inducement into the remedy for an unfair practice. It would therefore be wrong in law.

[314] In *Ramdath CA*, Feldman J.A. held that rescission or damages can be sought under s. 18 "with no inquiry into whether the consumer relied on the misrepresentation or was induced by it into entering the agreement", so that "common issues that are determinative of whether there is liability for a *Consumer Protection Act* claim can be certified". Feldman J.A. held (at paras. 86-89):

> The *Consumer Protection Act* came into force in 2005. It replaced the *Business Practices Act*, R.S.O. 1990, c. B.18, which was enacted in 1974. *The latter Act also contained a remedy of rescission and damages for an unfair practice where a consumer entered into an agreement following a false, misleading or deceptive representation*: ss. 2 and 4(1). *Unlike under the Consumer Protection Act, the Business Practices Act remedy was only available where the consumer was induced to enter into the agreement by the misrepresentation.*
>
> That inducement requirement was removed from the new Act. *A consumer who enters into an agreement following a misrepresentation is entitled to rescind the agreement and to claim damages with no inquiry into whether the consumer relied on the misrepresentation or was induced by it into entering into the agreement.*
>
> Reliance on a misrepresentation will not normally be a common issue in a class action, as it will depend on the individual history of each consumer …*By removing any requirement for reliance or inducement, common issues that are determinative of whether there is liability for a Consumer Protection Act claim can be certified, as they were in this case.*
>
> *The removal of the need for inducement or reliance is consistent with and facilitates the use of the Consumer Protection Act as a basis for class actions.* Section 8 of the *Consumer Protection Act* specifically contemplates class

> proceedings in respect of a consumer agreement and proscribes the ability to opt out of that right. The Supreme Court of Canada has recently endorsed the use of class actions to achieve the goals of similar legislation in Quebec: see generally *Richard v. Time Inc.*, 2012 SCC 8, [2012] 1 S.C.R. 265 and *Bank of Montreal v. Marcotte*, 2014 SCC 55, [2014] 2 S.C.R. 725. [Italics added.]

3.6(e) Analysis

3.6(e)(i) Is it settled law that restitutionary and nominal damages cannot be claimed by subscribers under s. 18?

[315] If the court accepts the facts as pleaded, it could find that Equifax engaged in "unfair practices" which could permit a rescission or damages claim under s. 18. Under s. 14 of the *Consumer Protection Act*, an unfair practice includes:

(i) a representation that the goods or services have sponsorship, approval, performance characteristics, accessories, uses, ingredients, benefits or qualities they do not have (s. 14(2)1),

(ii) a representation that the goods or services are of a particular standard, quality, grade, style or model, if they are not (s. 14(2)3), and

(iii) a representation using exaggeration, innuendo or ambiguity as to a material fact or failing to state a material fact if such use or failure deceives or tends to deceive (s. 14(2)14).

[316] The plaintiff alleges that Equifax made numerous falsehoods related to its protection of personal information, including that Equifax would act as a "trusted steward of personal information", who "maintains strict security safeguards when storing or destroying your personal information" and that Equifax "regularly review[s], test[s] and enhance[s] our systems to ensure they meet accepted industry standards".

[317] Equifax's position that restitutionary and nominal damages cannot be claimed by subscribers under s. 18 is the basis for both its "cause of action" objection for the Contract-Only Subclass and the "common issue" objection for the Combined Subclass. Equifax submits that since only compensatory damages can be sought by subscribers, the Contract-Only Subclass cannot bring an action for damages under s. 18 and the Combined Subclass cannot certify its damages claim under s. 18 as a common issue.

[318] I rely on my analysis for the Breach of Contract Objection set out above. I did not accept that it was settled law that subscribers could not seek restitutionary or nominal damages arising from the alleged breach of contract. For the same reasons, it is not settled law that damages for the alleged unfair practices are limited to expectation (compensatory) damages.

[319] Consequently, it is not settled law that (i) there is no cause of action under s. 18 for the Contract-Only Subclass, or (ii) the Combined Subclass would not be able to claim restitutionary or nominal damages under s. 18 as a common issue.

[320] For the above reasons, I reject Equifax's position on this issue.

3.6(e)(ii) Is it settled law that rescission is not available for current subscribers?

[321] Given my conclusion that the pleadings disclose a cause of action under s. 18 for both restitutionary and nominal damages, it is not necessary for me to review the rescission issue. Under s. 18(2), and the decision in *Ramdath CA* (at para. 94), a court has "'complete flexibility to award whatever damages would be appropriate at common law' including the restitutionary measure."

[322] Consequently, even if it were settled law that rescission was not available, I would certify PCI (xviii) since it is not plain and obvious that the restitutionary or nominal damages claim of all subscribers under s. 18 could not proceed.

[323] While the availability of a rescission claim is not necessary to my reasons, I still find that it is not plain and obvious that a rescission claim under s. 18(1) by those subscribers who remain Equifax customers will fail.

[324] Equifax submits that it is plain and obvious that rescission is not possible for current subscribers under s. 18(1) since its services "were fully performed and delivered during the substance of those contracts" and, as such, "cannot be restored in full – indeed at all".

[325] Equifax relies on the decision of Belobaba J. in *Ramdath v. George Brown College of Applied Arts and Technology*, 2012 ONSC 6173, 113 O.R. (3d) 531 ("*Ramdath SC*").[53] Belobaba J. held that "[o]n the facts of this case, rescission of the agreement is no longer possible because the educational program, whatever its value to the students, has been consumed and cannot be returned" (*Ramdath SC*, at para. 80).

[326] Owsianik relies on s. 18(1) which permits rescission of a contract if the court finds an unfair practice, which is defined under s. 14 of the *Consumer Protection Act* to be a false, misleading or deceptive representation.

---

[53] The decision in *Ramdath SC* was affirmed on appeal, 2013 ONCA 468, 307 O.A.C. 196. The *Ramdath CA* decision relied upon by Owsianik arose out of a subsequent decision of Belobaba J. in the same matter.

[327] Given that Equifax represented in its Privacy Policy that it was a "trusted steward of personal information", "maintains strict security safeguards when storing or destroying your personal information', and that "we regularly review, test and enhance our systems to ensure they meet accepted industry standards", Owsianik submits that for those subscribers who continue to pay for Subscription Products (in both the Contract-Only and Combined Subclasses), rescission may be available if an unfair practice can be established.

[328] For the reasons that follow, I agree with the position of the plaintiff.

[329] Each class member entered into a contract after or while Equifax allegedly engaged in an unfair practice (*e.g.* misrepresentation by Equifax as to services provided). Current subscribers remain in a contractual relationship with Equifax. In *Ramdath SC*, the students were no longer at the school and, as such, could not rescind the contracts.

[330] Consequently, it is not certain that a rescission claim will fail if existing Equifax subscribers can establish that they entered into an agreement after or while an unfair practice was occurring.

3.6(e)(iii) Conclusion on the Consumer Protection Legislation Objections

[331] For the above reasons, I find that it is not plain and obvious that the claims for restitutionary or nominal damages are not available. Consequently, there is a cause of action disclosed for the Contract-Only Subclass and a common issue for the Combined Subclass, both based on s. 18.

[332] Equifax's submissions require the court to accept that there is no restitution or nominal damage claim available for the subscribers, with any contractual claims limited to individual compensatory damages. As I did not accept that submission in the context of the Breach of Contract Objection, I do not accept the Consumer Protection Legislation Objections.

[333] Further, it is not plain and obvious that rescission is not available, although that conclusion is not necessary to certify PCI (xviii) given my findings above.

[334] For the above reasons, I certify PCI (xviii) as a common issue.[54]

[54] Having found that the breach of contract and consumer protection legislation claims disclose a cause of action for the Contract-Only Subclass, I necessarily reject the ancillary objections by Equifax that (i) there can be no Contract-Only Subclass under s. 5(1)(b) based on the lack of a cause of action, and (ii) there can be no common issue for the Contract-Only Subclass under s. 5(1)(c) on the basis that the Claim does not disclose a cause of action.

3.7 Objection 6: The Aggregate Damages Objection

[335] Pursuant to PCI (xix), the plaintiff seeks to certify the following question:

> Should an award of aggregate damages pursuant to s. 24(1) of the *Class Proceedings Act, 1992* be made?

[336] Equifax acknowledged, at the hearing, that an award for aggregate damages can be sought if the proposed common issues for intrusion upon seclusion were certified. Equifax also submitted in its factum:

> Admittedly, the Plaintiff's argument that an aggregated damages common issue should be certified in this case might be sound if the pleaded facts supported a claim for intrusion upon seclusion. In *Jones v. Tsige*, Sharpe J.A. wrote:[55]
>
> > In my view, damages for intrusion upon seclusion in cases where the plaintiff has suffered no pecuniary loss should be modest but sufficient to mark the wrong that has been done. I would fix the range at up to $20,000.
>
> While Justice Sharpe did not stipulate a lower limit, it was clearly implicit in the decision that it was higher than $0; in no case in which the tort was made out was the plaintiff to be denied an award of damages altogether. In essence, Sharpe J.A. established a general damages rule for intrusion upon seclusion analogous to that for the tort of defamation: general damages would be presumed in all cases, and only in fixing the quantum of those damages in an individual case was it necessary to consider the impacts on the particular plaintiff and the blameworthiness of the particular defendant's conduct.

[337] On this basis, the parties agreed at the hearing that the claim for aggregate damages could be certified as a common issue "for all or part of the damages claimed", if the court found the pleadings disclosed a cause of action for intrusion upon seclusion. Having done so, I certify the claim for aggregate damages on that basis.

[338] This approach is consistent with the decision of the court in *Good v. Toronto (Police Services Board)*, 2016 ONCA 250, 130 O.R. (3d) 241 ("*Good*"), in which the court held that a common issues judge could "determine that there was a base amount of damages that any member of the class (or subclass) was entitled to as compensation for breach of his or her [common law or *Charter*] rights" (*Good*, at para. 75).

---

[55] (*Jones*, at para. 87)

[339] This approach is also consistent with the decision of the court in *Daniells*, in which Ellies J. found a reasonable likelihood that aggregate damages could be assessed with respect to claims in negligence, breach of fiduciary duty, and breach of contract, even if individual assessments of damages may also be necessary (*Daniells*, at para. 66). Consequently, Ellies J. certified the question "[C]an an aggregate assessment be made of all or part of these damages?" (see *Daniells*, Appendix "C", p. 33 of the reasons).

[340] Consequently, I certify PCI (xix) on that basis. I adopt the language from *Daniells* and modify PCI (xix) as follows:

> Should an award of aggregate damages pursuant to s. 24(1) of the *Class Proceedings Act, 1992* be made for all or part of the damages claimed?

PART 4: ORDER AND COSTS

[341] I grant the motion and certify the proceeding as a class action, as set out in these Reasons. If the parties cannot agree on the terms of the order, they may return before me to settle its terms.

[342] If the parties are unable to agree on costs, Owsianik shall deliver a costs submission of no more than six pages (not including the costs outline) by January 14, 2020. Equifax shall deliver responding costs submissions of no more than six pages (not including the costs outline) by February 4, 2020. Owsianik may deliver a reply costs submission of no more than three pages by February 18, 2020 to address the responding costs submissions of Equifax.

GLUSTEIN J.

Date: 20191213

CITATION: Agnew-Americano v. Equifax Canada Co., 2019 ONSC 7110
COURT FILE NO.: CV-17-582551CP
DATE: 20191213

ONTARIO

SUPERIOR COURT OF JUSTICE

BETWEEN:

BETHANY AGNEW-AMERICANO and JANE DOE

Plaintiffs

AND:

EQUIFAX CANADA CO. AND EQUIFAX, INC.,

Defendants

REASONS FOR DECISION

Glustein J.

Released: December 13, 2019

SCHEDULE "A" - LIST OF PROPOSED COMMON ISSUES

Negligence

(i) Did the defendants, or either of them, owe a duty of care to Class Members in the collection, retention, use, disclosure and safeguard of personal information?

(ii) If so, did the defendants, or either of them, breach that duty?

Intrusion upon seclusion

(iii) Did the defendants, or either of them, invade, without lawful justification, the Class Members' private affairs or concerns by failing to take reasonable steps to ensure that Class Members' personal information was protected from appropriation by hackers?

(iv) Was the defendants' conduct intentional or reckless?

(v) Would a reasonable person regard the invasion as highly offensive, causing distress, humiliation or anguish?

Breach of privacy legislation

(vi) For class members resident in B.C., did the defendants, or either of them, violate section 1 of the *Privacy Act*, R.S.B.S. 1996, c. 373?

(vii) For class members resident in Manitoba, did the defendants, or either of them, violate section 2 of the *Privacy Act*, C.C.S.M. c. P.125?

(viii) For class members resident in Saskatchewan, did the defendants, or either of them, violate section 2 of the *Privacy Act*, R.S.S. 1978, c. P-24?

(ix) For class members resident in Newfoundland, did the defendants, or either of them, violate section 3 of the *Privacy Act*, R.S.N.L. 1990, c. P-22?

(x) For class members resident in Quebec, did the defendants, or either of them, violate Articles 35 and 37 of the *Civil Code of Quebec*, L.R.Q., c. C-1991?

Breach of contract

(xi) For Class Members that purchased Equifax Complete Advantage, Equifax Complete Premier, Equifax Complete Friends and Family or any other Equifax product offering credit monitoring and identity theft protection, was it a term of the contract that the defendants would maintain strict security safeguards when storing personal information?

(xii) Did the defendants comply with the contract by failing to apply a security patch made available in March 2017 until August 2017?

(xiii) For Class Members that purchased Equifax Complete Advantage, Equifax Complete Premier, Equifax Complete Friends and Family or any other Equifax product offering credit monitoring and identity theft protection, was it a term of the contract that the defendants would provide information to Members to help them minimize the risk of identity theft and to prepare them to respond to a real and/or suspected act of identity theft?

(xiv) Did the defendants comply with the contract?

Breach of consumer protection legislation

(xv) Did the defendants (or any of them) make false, misleading or deceptive representations within the meaning of the *Consumer Protection Act, 2002* or the Equivalent Consumer Protection Statutes (as defined in the Statement of Claim)?

(xvi) If so, were any such representations unconscionable?

(xvii) Is it in the interests of justice to disregard the requirement to give notice under the *Consumer Protection Act, 2002* or the Equivalent Consumer Protection Statutes (as defined in the Statement of Claim)?

(xviii) Are the class members, or any of them, entitled to rescission or damages under the *Consumer Protection Act, 2002* or the Equivalent Consumer Protection Statutes (as defined in the Statement of Claim)?

Aggregate damages

(xix) Should an award of aggregate damages pursuant to s. 24(1) of the *Class Proceedings Act, 1992* be made?

Punitive damages

(xx) Are the defendants, or either of them, liable to pay punitive or exemplary damages to the class members, having regard to the nature of their conduct, and if so, what amount?