**CITATION:** Grossman v. Nissan Canada, 2019 ONSC 6180
**COURT FILE NO.:** CV-18-00590402-CP
**DATE:** 20191029

***ONTARIO***
**SUPERIOR COURT OF JUSTICE**

B E T W E E N:

BORIS GROSSMAN and MICHAEL ARNTFIELD

Plaintiffs

and

NISSAN CANADA INC., c.o.b. as NISSAN CANADA FINANCE and INFINITY FINANCIAL SERVICES CANADA, NISSAN CANADA FINANCIAL SERVICES INC., SERVICES FINANCIERS NISSAN CANADA INC., and NISSAN NORTH AMERICAN, INC.

Defendants

**Proceeding under the *Class Proceedings Act, 1992***

**BEFORE:** Justice Edward P. Belobaba

**COUNSEL:** *Matthew Baer, Vadim Kats, Carlin McGoogan, Emily Assini and Christopher Du Vernet* for the Plaintiffs

*Michael Schafler, Kirsten Thompson and Chloe Snider* for the Defendants

**HEARD:** October 16 and 17, 2019

## MOTION FOR CERTIFICATION

[1] Data breaches involving the theft of personal information coupled with a ransom demand are becoming commonplace. In some cases, the loss of privacy and actual harm sustained is significant; in other cases, it is slight. But in almost every case a class action is sure to follow.

[2] As happened here.

[3] This is a motion for the certification of a class action arising from a data breach at Nissan Canada. The plaintiffs have sued several Nissan entities. For easier readability, I will refer to them as "the defendants" or "Nissan."

[4] The evidence suggests that very little in the way of private information was stolen and none of it was posted or otherwise made public. The damages sustained are so minimal, says Nissan, that a class action is not justified. The plaintiffs argue otherwise.

[5] It is not my job at this stage of the proceeding to assess the merits of the plaintiffs' claim. The merits will be determined in due course by way of summary judgment or trial. My only concern on this certification motion is to ensure that the procedural requirements set out in s. 5 of the *Class Proceedings Act*[1] ("CPA") have been satisfied.

[6] For the reasons set out below, I find that these requirements have been satisfied. The proposed action is certified as a class proceeding.

**Background**

[7] In December 2017, an unknown Nissan employee accessed a company data base that contained the personal information of thousands of customers who had financed the lease or purchase of their Nissan vehicle. The unknown employee emailed a "sample" of the stolen data to company executives and demanded the payment of a ransom.[2]

[8] Nissan refused to pay the ransom demand, posted news of the incident on its website, notified its 932,000 customers and offered one year of free credit monitoring.

[9] It appeared from the investigation that followed that the stolen data consisted of four uniform categories of personal information: the customers' name and address; the vehicle model and VIN; the terms of the lease/loan and monthly payment amount; and the customer's credit score. Initially, there was some concern about social insurance numbers, but this has now been investigated and there is no evidence that any SINs had been misappropriated.

[10] The first three categories - name and address, vehicle model and VIN, and the lease or loan terms - are personal information to be sure but they cannot fairly be described as private information. Your name and address are certainly not private; nor is the vehicle you drive or the VIN that is generally readable through the front window of the car. And vehicle lease or loan terms are publicly available in personal property registration data bases. The only item of personal information stolen by the unknown

---

[1] *Class Proceedings Act*, 1992, S.O. 1992, c. 6.

[2] According to its factum, Nissan's investigation concluded that this was "an inside job" by "an unknown employee who accessed the customer information and misused it to try to extort Nissan."

employee that could arguably fall with the category of private information is the customer's credit score. I agree with the plaintiffs that an individual's credit score can be highly revealing of one's financial situation and is something that a reasonable person would generally want to keep private.[3]

[11] Fortunately, almost two years later, there is no evidence that any of the stolen information has been made public or otherwise misused by the extortionist. There has been no activity on the dark web. There is no evidence of any breach-related fraud or identity theft. Only about four per cent of the 932,000 Canadian customers who received the notice letter have opted for the free credit monitoring.

[12] The plaintiffs understand that any actual or out of pocket losses are probably minimal to non-existent. Therefore, they rely primarily on "intrusion upon seclusion" a new privacy tort that was recognized by the Court of Appeal in 2012.[4] The advantage provided by the intrusion tort is that up to $20,000 in "symbolic" or "moral" damages can be awarded even if no financial or out of pocket loss has been sustained.[5]

**Analysis**

[13] The five requirements for the certification of a class action under s. 5(1) of the CPA are well known to counsel: a cause of action, an identifiable class, one or more common issues that will advance the litigation, a showing that a class action is the preferable procedure, and a suitable representative plaintiff with a workable litigation plan. The last four requirements only need a small amount of evidence – "some basis in fact" – in order to be satisfied.

**(1) Cause of action – section 5(1)(a)**

[14] The test under s. 5(1)(a) of the CPA is the same as the test on a motion to strike for no reasonable cause of action: assuming the facts pleaded to be true, is it plain and obvious that the claim has no reasonable prospect of success.[6]

[15] The plaintiffs have pleaded four causes of action: (i) the defendants' vicarious liability for the unknown employee's intrusion upon seclusion; (ii) breaches of provincial

---

[3] *Re PIPEDA Case Summary No. 63*, 2002 CarswellNat 5369.

[4] *Jones v Tsige,* 2012 ONCA 32.

[5] *Ibid.,* at paras. 71, 74-75 and 87.

[6] *Pro-Sys Consulting Ltd. v. Microsoft Corp.*, 2013 SCC 57 at para. 63; *R. v. Imperial Tobacco Canada Ltd.*, 2011 SCC 42 at para. 17.

privacy statutes; (iii) negligence; and (iv) breach of contract. Class counsel advised the court during the hearing that if the intrusion claim was certified, the statutory claims would not be pursued.

[16] I find that the cause of action requirement has been satisfied. Assuming the facts as pleaded are true, each of the three main claims - vicarious liability (for intrusion), negligence and breach of contract - have been sufficiently pleaded and disclose a cause of action.

[17] ***Vicarious liability for intrusion upon seclusion.*** The plaintiffs have properly pleaded the elements of the intrusion upon seclusion claim - an intentional or reckless invasion of private affairs or concerns that would be viewed by the reasonable person as highly offensive. The plaintiffs argued vicarious liability and referred to the appropriate case law in their factum, but vicarious liability was not pleaded in the statement of claim. However, the plaintiffs have now amended the statement of claim to correct this omission:

> 49. The Plaintiffs plead that one of the Defendants' employees, the identity of whom is unknown to the Plaintiffs (the "unknown employee"), gained access to the confidential information of the Defendants' customers which was stored in the Defendants' network or computer system and used it in the wrongful manner and for the wrongful purposes described elsewhere in this Claim.
>
> 50. At all material times, the unknown employee was an employee authorized to conduct business on behalf of the Defendants. This authority included accessing the information at issue for some purposes.
>
> 51. The Defendants collected confidential information of the Plaintiffs and class members, aggregated it and stored it on its network or computer system, and provided access to certain employees, including the unknown employee. By so doing, it created the risk that such information could be stolen or misused by those to whom access had been so given.
>
> 52. The Defendants furnished the unknown employee with the means to access its network or computer system including, without limitation, by providing whatever login name was required to access the confidential information, any passwords required to access the confidential information, and information regarding the location of the confidential information. By so doing, the Defendant materially increased the risk of theft or misuse of the confidential information by the unknown employee.
>
> 53. The Plaintiffs therefore plead that by operating its enterprise in this fashion, the Defendants created and materially increased the risk of theft of the confidential information by the unknown employee.

> 54. In such circumstances, the Defendants are vicariously liable for the intrusion upon seclusion committed by their unknown employee.

[18] The defendants have admitted that the unknown employee's access to the information in question was "authorized". In December 2018, Nissan updated its website to advise as follows:

> After a thorough investigation, NCF [Nissan Canada Financial] has concluded that this was not a case of unauthorized access. Indeed, at this time, NCF has no evidence of an intrusion by any unauthorized third party. Rather, NCF believes that this was a case of *authorized access* to the information and subsequent misuse for the purpose of making the extortion demand.[7]

[19] Whether the "subsequent misuse" argument is enough for Nissan to escape vicarious liability will be determined in due course at trial. At the certification stage, the question under s. 5(1)(a) of the CPA is much narrower - whether the vicarious liability claim has a reasonable prospect of success or is doomed to fail.

[20] In *Evans v. Wilson and Bank of Nova Scotia*,[8] this court allowed the vicarious liability claim on pleaded facts that were remarkably similar. A bank employee with authorized access to certain computer records misappropriated and misused confidential customer information. This court referred to the Supreme Court of Canada's decision in *Bazley v. Curry*[9] and concluded as follows:

> In this case, the Bank created the opportunity for Wilson [the employee] to abuse his power by allowing him to have unsupervised access to customers' private information without installing any monitoring system… [T]here is a significant connection between the risk created by the employer in this situation and the wrongful conduct of the employee …
>
> [T]he plaintiffs have pleaded … a complete lack of oversight by the Bank of its employees, including Wilson, with regard to improper access to personal and financial customer information. While the Bank itself was not directly involved in the improper access of customer information, vicarious liability "is strict, and does not require any misconduct on the part of the person who is subject to it": *Straus Estate v. Decaire*, 2011 ONSC 1157, 84 C.C.L.T. (3d) 141 at para. 49 …

---

[7] Emphasis added. I note that this notification also suggests that NCF, that is Nissan Canada Financial, is the locus of the data breach.

[8] *Evans v Wilson and Bank of Nova Scotia,* 2014 ONSC 2135.

[9] *Bazley v. Curry,* [1999] 2 S.C.R. 534.

> I find that it is not plain and obvious that the plaintiffs' claim that the Bank is vicariously liable for its employee's tort of intrusion upon seclusion would be unsuccessful.[10]

[21] Given the amended statement of claim, the defendants' acknowledgement that the unknown employee had "authorized access" and the decision in *Evans,* I cannot say that the plaintiffs' vicarious liability for intrusion claim has no chance of success and is doomed to fail. I find that this claim discloses a cause of action.

[22] ***Negligence.*** Each of the elements – duty and breach of care, causation and legally compensable loss - has been pleaded in detail. The negligence claim discloses a cause of action.

[23] ***Breach of contract.*** Because the data breach involved the Nissan defendants and not the independent dealers from whom the plaintiffs leased their cars, the plaintiffs had difficulty finding a legally binding agreement that would support their breach of contract claim against the defendants. The plaintiffs' initial submission was that the defendants' privacy policy as posted on their website created a contractual relationship with the dealer's customers. When it became apparent during the hearing that this submission would not succeed, the plaintiffs abruptly changed direction.

[24] The plaintiffs advised the court that the "common contract" was not the website privacy policy but rather the "credit application" that typically accompanied the lease agreement. The plaintiffs say the credit application was filled out and signed by every class member and was then forwarded to Nissan. A provision in this credit application arguably provided a similar promise of privacy protection.

[25] The statement of claim does not mention the credit application *per se* but a generous reading of the reference to "agreements to lease or purchase" could well include the requisite credit application. I need not dwell on this point because, in any event, the breach of contract claim does not survive the common issue analysis - the plaintiffs were unable to provide any evidence that the credit application was executed by every class member and was a common, class-wide contract.

[26] In sum, three causes of action clear the s. 5(1)(a) hurdle – vicarious liability for intrusion, negligence and breach of contract - but only two will clear the commonality hurdle under s. 5(1)(c): vicarious liability for intrusion and negligence.

**(2) Identifiable class – section 5(1)(b)**

[27] The next hurdle, section 5(1)(b) of the CPA, requires some evidence of an identifiable class of two or more persons.

---

[10] *Ibid.,* at paras. 22-26.

[28] The two plaintiffs, both of whom leased Nissan vehicles and whose personal information was listed in the data breach Sample, ask to be appointed representative plaintiffs for a national class defined as:

> All persons resident in Canada (including their estates, executors or personal representatives) excluding residents of Quebec who provided personal information to one or more of the Defendants or any of their affiliates or subsidiaries prior to December 11, 2017.

[29] The referenced date is the day that Nissan executives first learned of the data breach and ransom demand. Class members in Quebec are excluded because a separate class action, recently certified,[11] is proceeding in that province. Nissan sent a notice letter about the data breach to 932,000 customers. The Quebec proceeding includes the 302,000 class members that reside in that province. This proposed class action relates to the remaining 630,000 who live in the rest of Canada.

[30] In my view, the proposed class definition cannot be certified for at least two reasons. The first is that it is too broad. The class definition must be rationally connected to the proposed common issues in the context of the overall claim – namely, a data breach involving personal information that had been provided by customers who had financed the lease or purchase of their Nissan vehicle. The proposed class definition is too broad because it would also include current customers who had purchased a Nissan vehicle directly without leasing or financing.

[31] The proposed class definition would also include former Nissan customers who leased or purchased their vehicles years or decades ago, were no longer obliged under any lease or financing agreement and whose personal information was not disclosed in the data breach Sample. The class definition should reflect the reality that financing agreements for the lease or purchase of automobiles are rarely if ever longer than four or five years. An appropriate class period would therefore cover say five years and would begin on December 11, 2012.

[32] The second problem arises from another eleventh-hour revision by the plaintiffs. In their effort to establish commonality for the s. 5(1)(c) analysis and the proposed common issues ("PCIs"), class counsel abandoned their submission that the contents of the data breach were disparate and uncertain and, instead, advanced the (opposite but acccurate) submission that the *same* information was disclosed for all of the class members, namely the information items set out in the Sample. This revision is important because it means that this court can treat the four categories of personal/private information set out in the Sample as the *only* information at issue in this proceeding. That is, the Sample has now become the entirety of the data theft.

---

[11] *Levy v Nissan Canada Inc*., (Quebec Superior Court No. 500-06-000907-184, Sept. 19, 2019).

[33] Given this important revision, Nissan argues, understandably, that class membership should be limited to persons outside Quebec whose personal/private information was listed in the Sample. In other words, the class should be reduced from the 630,000 persons outside Quebec who received a notice letter about the data breach to the 183,000 person sub-set whose personal/private information was actually listed in the Sample and who therefore have a plausible damages claim.

[34] This is a sensible suggestion. However, the certified class definition must allow for reasonable self-identification by every class member.[12] The average class member at this point in the proceeding does not know if his or her information was listed in the Sample. But they do know if they received a notice letter from Nissan about the December 2017 data breach.

[35] Therefore, in my view, the most appropriate class definition for certification purposes is the following:

> All persons resident in Canada, including their estates, executors or personal representatives but excluding persons resident in Quebec, who (1) provided personal information to one or more of the defendants (or any of their affiliates or subsidiaries) when financing a lease or purchase of a Nissan vehicle over the five years ending on December 11, 2017 and (2) received a notice letter from Nissan about the December 2017 data breach.

[36] I note that in the parallel Quebec class action, Justice Gagnon certified a class definition that includes everyone who had received the notice letter.[13] A similar approach in this "rest of Canada" class action would obviously achieve a measure of consistency.

[37] However, because consistency may be the hobgoblin of small minds, I hasten to add the following. If Nissan can provide a more appropriate definition of class membership that satisfies the self-identification objective or if the upcoming discoveries suggest some other good reason to do so, Nissan may move to amend this class definition as soon as convenient. But for now, I am content to proceed with the class definition as just stated.

**(3) Common issues – section 5(1)(c)**

[38] Section 5(1)(c) of the CPA requires that the claims of class members raise common issues of fact or law that will move the litigation forward. For an issue to be a common issue, it need only be a substantial ingredient of every class member's claim and

---

[12] *Kalra v. Mercedes Benz,* 2017 ONSC 3795 at paras 35-36.

[13] *Levy, supra* note 11, at paras. 135-137.

its resolution must be a necessary component to the resolution of every class member's claim. A common issue 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. It is enough that the answer to the question does not give rise to conflicting interests among the class members. The underlying commonality question is whether allowing a proceeding to continue as a class proceeding will avoid duplication of fact-finding or legal analysis.[14]

[39] In recent years, some judges, myself included, have tried to clarify the test for commonality. Is it a two-step test (some evidence that the proposed common issue exists and some evidence of commonality) or just a one-step test (some evidence of commonality): see, for example, my ruminations about the state of the law in *Kalra v. Mercedes Benz*[15] and *Kaplan v. Casino Rama*.[16] In my opinion, given what was said by the Supreme Court of Canada in *ProSys Consultants,*[17] the governing test is now a single-step question: is there some evidence of class-wide commonality, that is some evidence that the proposed common issue can be answered on a class-wide basis?

[40] On this motion, counsel on both sides were content to use the one-step test. The dispute between the parties was whether there was some evidence of commonality.

[41] The plaintiffs ask that seven PCIs be certified: vicarious liability for intrusion upon seclusion; breach of provincial privacy statutes; breach of the duty and standard of care; breach of contract; aggregate damages; individual damages; and punitive damages.

[42] The plaintiffs' change of direction during the hearing of the motion that the personal/private information misappropriated by the data thief was the *same* in every case (and that the entirety of the stolen information was contained in the Sample) made the commonality argument easier for at least three of the PCIs: vicarious liability for intrusion, negligence and aggregate damages.

[43] I will consider each of the PCIs in turn.

[44] The PCI about vicarious liability for intrusion upon seclusion is certified exactly as it was in *Evans.*[18] Common Issue No. 1 will read as follows:

---

[14] *Western Canadian Shopping Centres Inc. v. Dutton,* 2001 SCC 46, at para. 39; *Pro-Sys Consulting, supra,* note 6, at para. 108.

[15] *Kalra, supra,* note 12, at paras. 41-47.

[16] *Kaplan v Casino Rama,* 2019 ONSC 2025, at paras. 47-54.

[17] *ProSys Consultants, supra*, note 6, at para. 110.

[18] *Evans, supra,* note 8, at para. 96.

> (1) Is the unknown employee liable for the tort of intrusion upon seclusion and if so, should the defendants be held vicariously liable?

[45] This common issue can be answered on a class-wide basis. Given the sameness of the data breach, there is no part of this question that requires an individualized analysis. Whether the intrusion upon seclusion was intentional (or reckless) or resulted in an unlawful invasion of private affairs or concerns (i.e. the credit scores) or would be viewed by a reasonable person as highly offensive[19] are questions that can be answered in common across the class.

[46] The defendants submit that the second element of the intrusion tort, the invasion of one's private affairs or concerns, requires individualized assessments because every person's sensitivities about the release of say their credit score would be different. I do not agree. I see no requirement for any such "subjective" analysis in the *Jones v Tsige* decision. To the contrary, the Court of Appeal made clear that it was adopting the formulation in the American *Restatement (Second) of Torts (2010)*, a formulation that said nothing about subjective or individualized perspectives:

> One who intentionally intrudes, physically or otherwise, upon the seclusion of another or his private affairs or concerns, is subject to liability to the other for the invasion of his privacy, if the invasion would be highly offensive to a reasonable person.[20]

[47] The Court of Appeal also made clear that subjective or individual "sensitivities" were not to be considered and that the determining norm was the objective assessment of the reasonable person:

> 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.[21]

[48] I therefore conclude that the intrusion part of Common Issue No. 1 can be objectively answered on a class-wide basis through the lens of the reasonable person. The second part of the common issue - whether the defendants should be held vicariously liable – requires the court to consider the actions of the unknown employee and the

---

[19] *Jones, supra,* note 4, at para. 71.

[20] *Ibid.,* at para. 70.

[21] *Ibid.,* at para. 72. Emphasis added.

defendants. It does not require any individualized assessment of the actions of the class members. The first PCI is therefore certified as a common issue.

[49] As already noted, the plaintiffs have advised that if the vicarious liability for intrusion question is certified as a common issue, the PCI relating to the privacy laws in British Columbia, Saskatchewan, Manitoba and Newfoundland-Labrador will not be pursued. I hasten to add, however, that the common issue about vicarious liability for intrusion may still be advanced on behalf of the class members who live in the four provinces with privacy statutes.[22]

[50] The PCI about the negligence claim and, specifically, the questions about duty and standard of care are certified as follows:

> (2)(a) Did the defendants owe the class a duty of care? If so, what duty of care was owed to the class?
>
> (b) What was the applicable standard of care for each defendant? Did the defendants breach the applicable standard of care?

[51] The applicable duty and standard of care in the context of a case involving the data theft of personal information is set out in the federal PIPEDA statute:

> The nature of the safeguards will vary depending on the sensitivity of the information that has been collected, the amount, distribution, and format of the information, and the method of storage. More sensitive information should be safeguarded by a higher level of protection.[23]

[52] In *Kaplan,* I refused to certify the duty and standard of care questions because "[t]he type and amount of personal information posted online by the hacker varied widely from individual to individual."[24] Here, because the same items of information were stolen by the data thief, the duty and standard of care will be the same for every individual. The duty and standard of care questions can be answered in common on a class-wide basis and are therefore certified as set out above.

[53] The PCI about breach of contract is not certified. Put simply, the plaintiffs were unable to provide any evidence that the credit application, referenced above in my discussion of s. 5(1)(a), was a common contract that had been executed by all or even any of the class members. Given this lack of commonality, the breach of contract question cannot be answered on a class-wide basis.

---

[22] See *Evans, supra,* note 8, at para. 26.

[23] *Personal Information Protection and Electronic Documents Act,* S.C. 2000, c. 5, Sched. 1, s. 4.7.2.

[24] *Kaplan, supra,* note 16, at para. 64.

[54] The PCI about aggregate damages is certified as follows:

> (3) If the answer to No. (1) is yes, can the class members' claim for symbolic or moral damages be assessed in whole or in part in the aggregate and, if so, what is the amount of the aggregate damages?

[55] The basis for the aggregate damages question is the proposition that if Nissan is found vicariously liable for the unknown employee's intrusion upon seclusion, there may be some common (base) amount that "objectively" could be awarded to every class member as symbolic or moral damages relating to the disclosure of their credit score. The amount of the common award may well be modest because the credit scores were not posted or otherwise made public. However, (tracking the language in s. 24 of the CPA) this base amount could be reasonably determined without proof by individual class members.

[56] The payment of the same base amount to every class member under the rubric of s. 24 of the CPA was approved by the Court of Appeal in *Good v. Toronto Police Services Board.*[25] The decision in *Good* was followed in *Daniells*[26] where this court certified the aggregate damages issue to potentially allow the payment of a base amount in the context of a privacy breach. This makes sense where, as here, every class member's privacy was breached in the same way.

[57] I am well aware that when aggregate damages are certified as a common issue, the plaintiff is generally required to provide "a plausible expert methodology that is capable of measuring the actual loss sustained by the class members on a class-wide basis."[27] The plaintiffs say that this methodology is set out in their Litigation Plan. Unfortunately, no such methodology can be found in the Litigation Plan. Nonetheless, I am still prepared to certify the aggregate damages question as a common issue. I do so because if Common Issue No. I is answered in the affirmative, the award of a base amount for symbolic or moral damages as based on the trial judge's objective determination is not something that requires an expert methodology.

[58] The plaintiffs also propose common issues that ask about each class member's damages and about overall punitive damages. The PCI that asks about the damages to which "each class member" is entitled cannot be certified because, as the quoted phrase suggests, the PCI cannot be answered on a class-wide basis.

---

[25] *Good v. Toronto Police Services Board,* 2016 ONCA 250 at para. 81.

[26] *Daniells v. McLellan,* 2017 ONSC 3466.

[27] *Kalra, supra* note 12, at para. 48. *Kaplan, supra* note 16, at para 84.

[59] The first part of the PCI that asks about the entitlement to punitive damages can be certified as a common issue because it depends on the conduct of the defendants not the class members and can thus be answered on a class-wide basis The second part of the PCI that asks about the "amount" of punitive damages that should be paid by the defendants is best left to the trial judge.[28]

[60] In sum, four PCIs are certified as common issues – vicarious liability for intrusion upon seclusion, duty and standard of care, aggregate damages, and the entitlement to punitive damages.

**(4) Preferable procedure – section 5(1)(d)**

[61] Section 5(1)(d) of the CPA requires the plaintiff to provide some basis in fact that a class proceeding is the "preferable procedure for the resolution of the common issues." The plaintiff must provide some evidence that: (1) a class proceeding would be a fair, efficient and manageable method of advancing the claim, and (2) that it would be preferable to any other reasonably available means of resolving the class members' claims. The preferability analysis must be conducted through the lens of the three principal goals of class actions, namely judicial economy, behavior modification, and access to justice.[29]

[62] I agree with the defendants that the goal of behavioral modification has already been achieved. The Office of the Information and Privacy Commissioner of British Columbia conducted its own investigation and concluded in its Report that it was "satisfied that [Nissan] has made every reasonable effort to mitigate any potential harm to the affected individuals that may result from the breach and that appropriate steps have been taken to prevent future breaches."

[63] I also agree with the defendants that if the duty and standard of care questions were the only common issues certified herein, the preferable redress procedure would be individual tort claims in Small Claims Court. The answers to the duty and standard of care questions are self-evident. Their resolution would not advance the litigation in any significant fashion and individual trials would still be needed to determine the economic losses. In terms of fairness and efficiency, the Small Claims Court would be the more sensible venue to adjudicate what would be, at most, a handful of negligence claims for very modest out of pocket losses.

---

[28] In *Whiten v. Pilot Insurance Co.,* 2002 SCC 18, the Supreme Court made clear at para. 94 that punitive damages should only be awarded if compensatory damages are insufficient to punish the defendant. In the class action context, the total compensation amount will not be known until the common issues and individual claims have been fully decided by the trial judge.

[29] *Hollick v. Toronto (City)*, 2001 SCC 68, at para. 27; *Kalra, supra* note 12, at para. 75.

[64] Here, however, I have also certified the vicarious liability/intrusion issue and the related aggregate (base amount) damages issue. These are more contentious questions and their answers would not only advance but probably end the litigation.[30] A class proceeding would allow both the vicarious liability and the aggregate damages issues to be decided once and for all on a class-wide basis.

[65] In sum, a class proceeding that would decide Common Issues Nos. 1 and 3 (and also No. 2) is justified as preferable on the two remaining grounds: access to justice and judicial economy.

[66] The preferability requirement is satisfied.

**(5) Suitable representative plaintiff – section 5(1)(e)**

[67] The final requirement for certification is a representative plaintiff who would adequately and fairly represent the interests of the class, and who does not have a conflict of interest with respect to the common issues.

[68] The proposed representative plaintiffs, Messrs. Grossman and Arntfield, each leased a Nissan vehicle. Their personal/private information was misappropriated in the data breach. Both have sworn that they would prosecute the action in favour of the class. They have filed a litigation plan that sets out a workable method of advancing the proceeding on behalf of the class. Neither has a conflict of interest with any of the other class members.

[69] The requirements of s. 5(1)(e) are satisfied.

**Disposition**

[70] The motion for certification is granted.

[71] Messrs. Grossman and Arntfield are appointed as the representative plaintiffs.

[72] The class definition is revised to read as follows:

> All persons resident in Canada, including their estates, executors or personal representatives but excluding persons residents in Quebec, who (1) provided personal information to one or more of the defendants (or any of their affiliates or subsidiaries) when financing a lease or purchase of a Nissan vehicle over the five years ending on December 11, 2017 and

---

[30] If the defendants prevail on these issues, the case would be over. If the class prevails, follow-up individual trials to recover symbolic damages in excess of the base amount would be highly unlikely. Either way the litigation would end.

(2) received a notice letter from Nissan Canada about the December 2017 data breach.

[73] The following questions are certified as common issues:

(1) Is the unknown employee liable for the tort of intrusion upon seclusion and if so, should the defendants be held vicariously liable?

(2) (a) Did the defendants owe the class a duty of care? If so, what duty of care was owed to the class?

(b) What was the applicable standard of care for each defendant? Did the defendants breach the applicable standard of care?

(3) If the answer to Common Issue No. 1 is yes, can the class members' claim for symbolic or moral damages be assessed in whole or in part in the aggregate and if so, what is the amount of the aggregate damages?

(4) Are the class members entitled to punitive damages?

[74] Counsel shall prepare a draft Order in the form contemplated by s. 8 of the CPA.

**Costs**

[75] The plaintiffs have prevailed on this motion for certification. However, it does not follow that they are automatically entitled to costs. The plaintiffs made several significant changes in the pleadings and in the formulation and presentation of their submissions. Some of the changes were made during the hearing and others in response to my questions after the hearing was over. I am sure that the defendants will have much to say about these revisions and their impact on the amount and direction of any costs award.

[76] If the parties are unable to agree on costs, I would be pleased to receive brief written submissions from the plaintiff within 14 days and from the defendants within 14 days thereafter.

[77] I am obliged to counsel on both sides for their assistance.

Justice Edward P. Belobaba

**Released:** October 29, 2019