CITATION: Kaplan v. Casino Rama, 2019 ONSC 2025
COURT FILE NO.: CV-16-564080-CP
DATE: 20190507

ONTARIO
SUPERIOR COURT OF JUSTICE

Between:

Leonid Kaplan, Ronald Goodfellow, Jennifer Alton, Thomas Champagne and Cheryl Jane Mizzi

Plaintiffs

and

Casino Rama Services Inc., CHC Casinos Canada Limited, Penn National Gaming Inc. and Ontario Lottery and Gaming Corporation

Defendants

Proceeding under the *Class Proceedings Act, 1992*

BEFORE: Justice Edward P. Belobaba

COUNSEL: *Theodore P. Charney, Tina Q. Yang and David Robins* for the Plaintiffs

Catherine Beagan Flood, Nicole Henderson, Jessica Lam and Christopher DiMatteo for the Defendants

HEARD: November 7 and 8, 2018 and March 28, 2019

Motion for Certification

[1] Two and a half years ago, in November 2016, Casino Rama was targeted in a cyber-attack. An anonymous hacker accessed the Casino's computer system and stole

personal information relating to customers, employees and suppliers. When ransom demands proved futile, the hacker posted the stolen data on the internet. Just under 11,000 people had some personal information posted online.

[2] The Casino contacted all appropriate authorities, took steps to close down the two websites that contained the stolen information, notified the thousands of customers, employees and suppliers potentially affected by the security breach and offered free credit monitoring services for one-year to many of them.

[3] Fortunately, some two and half years later, there is no evidence that anyone has experienced fraud or identity theft as a result of the cyber-attack. There is no evidence that anyone has sustained any compensable financial or psychological loss.

[4] Nonetheless, the plaintiffs insist on exercising their right to propose a class action. Class counsel candidly concedes that the most likely outcome, if they are successful, is the recovery of nominal damages for breach of contract – that is breach of certain alleged privacy agreements.

The parties

[5] The plaintiffs propose five representatives for this class action:

(i) *Leonid Kaplan* - member of the Casino's loyalty program, the Players Passport Club – nothing posted online – no financial loss;

(ii) *Cheryl Jane Mizzi* - member of the Players Passport Club - nothing posted online - no financial loss;

(iii) *Thomas Champagne* - joined the OLG's "self-exclusion program" – was required to provide driver's licence information and photo to the OLG – nothing posted on line – concerned about the "sensitive" nature of the information that he is a member of the "self-exclusion program" - didn't trust the Casino and wanted more than just one-year of credit monitoring, so he purchased a multi-year package on his own;

(iv) *Ronald Goodfellow* - member of the Players Passport Club – his name and postal code were posted online - no financial loss;

(v) *Jennifer Alton* - former part-time Casino employee – her name and address, date of birth, social insurance number, bank account details and photo were posted online - no financial loss.

[6] Only two of the proposed representatives had personal information posted online, Mr. Goodfellow and Ms. Alton. While each of the proposed representative plaintiffs stated in their affidavits that they have been monitoring their financial accounts for

suspicious activity, none of them say that they have experienced any fraud or identity theft as a result of the cyber-attack. Each of them were "shocked and concerned" and generally upset when they first learned about the cyber-attack but there is no evidence that any of them sustained any compensable financial loss or psychological harm as a result of the November 2016 hacking episode.

[7] The defendants can be briefly described as follows. Casino Rama at all material times was operated by CHC Casinos Canada Limited under an agreement with the OLG. Casino Rama Services, a wholly owned subsidiary of Penn National Gaming Inc., was the employer of all the employees at Casino Rama, some of were under a collective agreement. CHC is subject to the oversight of the OLG, and both CHC and the OLG are subject to the oversight of the Alcohol and Gaming Commission of Ontario (no longer a defendant in this proposed proceeding.)

Recent developments

[8] ***The second ransom demand.*** On August 19, 2018, the Casino received a new ransom demand from the hacker threatening to release additional stolen information if the ransom was not paid. However, the private link to "sample data" that was provided, revealed no new information – the sample consisted entirely of documents or parts of documents that had already been posted in November 2016. The ransom was not paid and, as it turned out, no further information, not even the "sample data", was posted online. In short, there is no evidence that the hacker is sitting on new or additional information that was not already posted in November 2016.

[9] ***The report of the Information and Privacy Commissioner.*** On November 9, 2016, within a few days of the hack, the OLG notified the Office of the Information and Privacy Commissioner of a possible privacy breach under provincial privacy law. An IPC staff investigator conducted an investigation and released her findings in a Report dated January 30, 2019. The IPC investigator concluded as follows:

(i) The CRR (Casino Rama Resort) did not have reasonable security measures in place to prevent unauthorized access to records of personal information of CRR patrons and individuals registered for OLG's self-exclusion program. However, since the breach, CRR has taken steps to address the gaps in its systems and processes. Although I am generally satisfied with CRR's response to the breach in this regard, this report makes additional comments to address some specific shortcomings;

(ii) The OLG did not have reasonable contractual and oversight measures in place to ensure the privacy and security of the personal information of CRR patrons and OLG self-exclusion registrants. This report also makes recommendations to address these shortcomings.

[10] I am advised by counsel that the IPC report did not address any possible statutory violations involving the employees' personal information because that mandate falls within federal privacy law and the office of the federal privacy commissioner. The latter has not yet released its report.

[11] The provincial IPC report also noted the following (the second part of this finding is contested by the Casino defendants):

> While only information relating to CR employees and CR patrons was released online by the hacker ... OLG and CHC have not been able to determine whether any additional information beyond what was released online was in fact stolen by the hacker.

[12] The impact of the IPC report for the purposes of this proposed class action is this. The finding that the Casino and the OLG did not have reasonable security measures in place to prevent unauthorized access to the personal information of Casino patrons or individuals registered for OLG's self-exclusion program is helpful to the plaintiffs but not determinative of legal liability. The latter requires a more careful analysis, as explained in detail below.

[13] The suggestion that "additional information" may have been stolen and could still be posted online by the hacker or his associates in the months or years ahead is plausible but not persuasive. Given the passage of two and a half years, and the fact that the second ransom demand revealed no such additional information, it is more likely than not that the risks of any informational misuse from the November 2016 hacking episode are minimal to non-existent. And, if any additional information is posted and misused in the months ahead, causing compensable monetary loss or psychological harm, a further class action can be commenced. In other words, there is no need to be concerned at this time about possible future claims.

Analysis

[14] I now turn to the certification analysis. The fact that there are no provable losses and that the primary culprit, the hacker, is not sued as a defendant makes for a very convoluted class action. Class counsel find themselves trying to force square (breach of privacy) pegs into round (tort and contract) holes. And defence counsel, not surprisingly, takes issue with all five of the certification requirements as set out in s. 5(1) of the *Class Proceedings Act* ("CPA").[1]

---

[1] S.O. 1992, c. 6.

[15] The defendants say there are no viable causes of action; the class definition is over-broad and unprincipled; there is no commonality in any of the proposed common issues; a class action is not the preferred procedure; and the proposed representative plaintiffs are inadequate and unsuitable.

[16] There is much to be said for many of the submissions. However, the single most compelling submission advanced by the defendants relates to s. 5(1)(c) of the CPA and the absence of commonality. I agree with this submission. In my view, this proposed class action collapses in its entirety at commonality.

[17] I will deal briefly with the cause of action and the class definition requirement under ss. 5(1)(a) and (b) of the CPA but I will focus primarily on the s. 5(1)(c) stage of the analysis and the plaintiffs' failure to show commonality in any of the proposed common issues.

[18] First, a quick look at ss. 5(1)(a) and 5(1)(b).

Causes of action

[19] The plaintiffs advance five causes of action: negligence, breach of contract, intrusion upon seclusion, breach of confidence and 'publicity given to private life.' If pressed, I would find viable causes of action in negligence, breach of contract and intrusion upon seclusion. However, I would find it plain and obvious that breach of confidence and publicity given to private life are doomed to fail and should be struck.

[20] ***Negligence.*** Although the statement of claim leaves much to be desired (too many bald assertions, not enough material facts), I am prepared to agree with the plaintiffs that it is not plain and obvious that the negligence claim is doomed to fail.

[21] The defendants are correct in their submission that the mere possibility that class members may experience identity theft or fraud at some time in the future, "falls squarely within the field of "speculation"[2] and does not give rise to compensable damages. The risk of some harm materializing in the future "is not actionable in the absence of a present injury."[3] The defendants are also correct to say that damages for mere frustration, anxiety and inconvenience are not compensable as a matter of law.[4]

---

[2] *Mazzonna v. DaimlerChrysler Financial Services Canada Inc.*, 2012 QCCS 958 at para. 66.

[3] *Ring v. Canada (Attorney General)*, 2010 NLCA 20 at paras. 52, 54 and 58.

[4] *Mustapha v. Culligan of Canada Ltd.*, 2008 SCC 27.

[22] Here, however, the pleadings set out certain allegations of loss that have been judicially accepted as compensable in breach of privacy class actions – in particular, damage to credit reputation, the costs of credit monitoring, costs incurred in preventing or rectifying identity theft or fraud and out-of-pocket expenses.[5]

[23] Here, as well, the pleadings go beyond everyday frustration and anxiety and allege mental distress that is "serious and prolonged", a psychological harm that is compensable under the law.[6]

[24] In sum, I am not prepared to find that the negligence claim is doomed to fail.

[25] ***Breach of contract.*** Nor am I prepared to find that the breach of contract claim as pleaded is doomed to fail. I agree with the defendants that a company's recitation of a privacy policy whose scope and content is determined solely by federal or provincial privacy law does not generate an enforceable consumer agreement. As recognized in *John Doe*[7] and *Broutzas*,[8] courts generally do not enforce agreements that simply repeat without more pre-existing statutory duties.[9]

[26] Here, however, there is more. The plaintiffs allege breach by the defendants of their own privacy policy (not just the one that was statutorily-mandated) and breach of "industry standards" whatever that may mean.

[27] I am therefore inclined to find that the breach of contract claim discloses a viable cause of action under s. 5(1)(a) of the CPA.

[28] ***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,*[10] 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.

---

[5] *Hynes v. Western Regional Integrated Health Authority,* 2014 NLTD 137 at paras. 27-30; *Evans v. Wilson,* 2014 ONSC 2135, at paras. 49-52.

[6] *Mustapha, supra,* note 4, at para. 9.

[7] *R. v. John Doe,* 2016 FCA 191.

[8] *Broutzas v. Rouge Valley Health System,* 2018 ONSC 6315.

[9] *John Doe, supra,* note 7, at para. 46; *Broutzas, supra,* note 8, at para. 217.

[10] *Jones v. Tsige,* 2012 ONCA 32 at para. 71.

[29] However, given the comments of the B.C. court in *Tucci*[11] and this court in *Bennett*[12] and *Equifax Canada*[13]- 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.

[30] ***Breach of confidence.*** The elements of this tort are that (a) the plaintiff conveyed confidential information to the defendant; (b) did so in confidence and (c) the defendant then "misused" the information "to the detriment of the party communicating it".[14]

[31] Unless the word "misuse" is distorted out of all shape and meaning, the defendants' failure to prevent the cyber-attack is not a "misuse" of confidential information within the meaning of the breach of confidence tort.

[32] The breach of confidence claim is doomed to fail.

[33] ***Publicity given to private life.*** To the extent that the tort of publicity given to private life even exists in Ontario — there is no appellate authority yet to this effect — it only captures intentional, deliberate publications of private material. *Jane Doe 464533 v. D.(N.),*[15] the only Ontario case expressly recognizing this tort, identified the following three elements: (i) the defendant gives publicity to a matter concerning the private life of another; (ii) the matter publicized, or the act of publication, would be highly offensive to a reasonable person and (iii) is not of legitimate concern to the public.[16]

[34] As the American *Restatement on Privacy* makes clear, the defendant is liable only if he or she makes "public [the private matter] by communicating it to the public at large or to so many persons that the matter is regarded as substantially certain to become one of public knowledge."[17] Here it is clear that the party that would be liable for publishing the

---

[11] *Tucci v. Peoples Trust Company,* 2017 BCSC 1525, at paras. 2, 152 and 257.

[12] *Bennett v. Lenovo*, 2017 ONSC 1082 at paras. 20 and 23.

[13] *Bethany Agnew-Americano v. Equifax Canada Co.* 2018 ONSC 275 at paras. 144-63.

[14] *Lac Minerals Ltd. v. International Corona Resources Ltd.*, [1989] 2 S.C.R. 574 at para. 10, citing *Coco v. A. N. Clark (Engineers) Ltd.*, [1969] R.P.C. 41 (Ch.) at 47.

[15] *Jane Doe 464533 v. D.(N.),* 2016 ONSC 541 at para. 45.

[16] *Ibid.,* at para. 46

[17] *Restatement, Privacy*, "Invasion of Privacy" (Division 6A, c. 28A, §652D), at para. A.

class members' information would not be any of the defendants. It would be the hacker. The plaintiffs provide no authority for the proposition that a defendant could be liable, not for actually publicizing private facts about the plaintiff, but for allegedly failing to prevent a third party from doing so.

[35] The publicity given to private life claim is doomed to fail.

[36] In sum, the three possibly viable claims are negligence, breach of contract and intrusion upon seclusion.

Class definition

[37] The plaintiffs suggest a proposed class defined that is overbroad and imprecise:

> All persons residing in Canada, excluding the defendants and the defendants' executives:
> a. to whom Casino Rama provided notice of the Breach by email, lettermail or telephone;
> b. whose Personal Information was posted online in one of the two "data dumps" on November 11 and November 21, 2016; or
> c. whose Personal Information was contained on one of the two servers which was accessed in the Breach.

[38] Given my conclusion that this proposed class action collapses in its entirety at the requirement of commonality under s. 5(1)(c), there is no need to dwell on the class definition under s. 5(1)(b). Except to make the following point.

[39] I agree with the defendants that the class definition cannot include the Casino's unionized employees. In my view, this court lacks jurisdiction over the contractual claims of the approximately 1,690 Casino employees whose employment is governed by a collective agreement dated January 24, 2016. The union representing these employees, Unifor Local 1090, has already reserved its rights to file grievances on behalf of employees who allege damages from the cyberattack under the procedure contained in article 37 of this collective agreement.

[40] The Ontario *Labour Relations Act*[18] mandates final and binding arbitration of "all differences…arising from the interpretation, application, administration or alleged violation" of a collective agreement.[19] Here, the gravamen of the plaintiffs' claims

---

[18] S.O. 1995, c. 1, Sch. A,

[19] *Ibid.*, s. 48(1).

relating to unionized employees is that the Casino breached an obligation to safeguard employee personal information. Whether framed in contract or in tort, the essential character of these claims relates to an important aspect of the employment relationship between the Casino and its employees and therefore arises from the collective agreement.[20] Any breach of privacy claims by these employees fall within the exclusive jurisdiction of the Ontario Labour Relations Board.[21]

[41] In *Bisaillon v. Concordia University*,[22] the Supreme Court of Canada held that it would undermine the exclusive jurisdiction of labour arbitrators, and the union's monopoly on representation of unionized workers for a Superior Court to certify a class action giving a representative plaintiff (instead of the union) the authority to represent unionized employees in relation to their conditions of employment.[23] The Supreme Court dismissed the certification motion in that case even though some of the proposed class members were non-unionized employees.[24]

[42] Returning to the class definition, the defendants say the plaintiffs' class definition is over-broad and instead suggest the following:

> All persons residing in Canada, excluding the defendants and the defendants' executives and members of Unifor Local 1090, whose information was stolen from Casino Rama's computer network in the Breach [as defined in the statement of claim].

[43] The defendants go on to say that even this narrower definition is still too broad because it would include individuals whose stolen information was personal (such as one's name or postal code) but not private or confidential.

[44] My only contribution to the class definition question is to make clear my agreement with the defendants that at the very least the class definition should exclude the unionized employees. The plaintiffs have advised that they are no longer making any claims on behalf of vendors or suppliers. The class definition may therefore continue to include the non-unionized employees, the members of the self-exclusion program and the members of the Players Passport club.

---

[20] *New Brunswick v. O'Leary*, [1995] 2 S.C.R. 967 at para. 6.

[21] *Supra*, note 18, s. 48(1); *Weber v. Ontario Hydro*, [1995] 2 S.C.R. 929 at paras. 55-63.

[22] *Bisaillon v. Concordia University*, 2006 SCC 19.

[23] *Ibid.*, at paras. 22, 24 and 25.

[24] *Bisaillon, supra*, note 22, at paras. 56 and 63-64.

[45] I come now to commonality. As already noted, it is at this stage that the proposed class action collapses in its entirety.

Proposed common issues

[46] The plaintiffs ask that 30 proposed common issues ("PCIs") be certified. They have been grouped under five heads: negligence, breach of contract, breach of confidence, privacy torts and damages and administration. I have attached the PCIs in the Appendix for easy reference.

[47] Before turning to the analyses of the PCIs, it is essential to agree on the appropriate test: is the "some basis in fact" test that applies in the s. 5(1)(c) analysis a two-step test (some evidence of both the existence of the PCI *and* the commonality of the PCI) or is it a one-step test (some evidence of just the commonality of the PCI)?

[48] For many years, class action judges applied a two-step test – we required some evidence that the proposed common issue actually exists (that is "...some evidentiary basis indicating that a common issue *exists* beyond a bare assertion in the pleadings"[25]) *and* some evidence that the proposed issue can be answered in common across the entire class (that is, some evidence of class-wide commonality).

[49] In 2013, in *ProSys Consultants*,[26] however, the Supreme Court eliminated the first step of the two-step approach. The Supreme Court said this: "In order to establish commonality, evidence that the acts alleged actually occurred is not required."[27]

[50] The impact of this pronouncement was largely ignored by lower court judges. I first grappled with this issue in 2015 in *Dine v Biomet*.[28] I considered what was said by the Supreme Court in *ProSys* but eventually concluded that the issue did not have to be resolved in the matter before me because the plaintiff had satisfied both steps of the commonality analysis.[29]

---

[25] *Fulawka v. Bank of Nova Scotia,* 2012 ONCA 443, at para. 79 ("...some evidentiary basis indicating that a common issue *exists* beyond a bare assertion in the pleadings.")

[26] *ProSys Consultants Ltd. v. Microsoft Corp.*, 2013 SCC 57.

[27] *Ibid.*, at para. 110.

[28] *Dine v. Biomet,* 2015 ONSC 7050.

[29] *Ibid.*, at note 9.

[51] Two years later, in *Kalra v. Mercedes Benz*[30] I returned to the discussion, this time fully embracing the Supreme Court's "one step" pronouncement. I set out my reasoning as follows:

> *The "some basis in fact" test.* I have long believed that the "some basis in fact" test was a two-step test: that the plaintiff must show some evidence of the existence of the proposed common issue *and* some evidence that the proposed common issue has class-wide commonality.[31]
>
> ...
>
> [However] I have come to understand that the Supreme Court's reminder ... that the "some basis in fact" test in the context of the common issues is only a one-step process is a reminder that should be taken literally:
>
> > In order to establish commonality, evidence that the acts alleged actually occurred is not required. Rather, the factual evidence required at this stage goes only to establishing whether [the common issues] are common to all the class members.[32]
>
> I am [now] persuaded that it is time to retire the two-step approach and focus only on class-wide commonality. The plaintiff only has to show some evidence of commonality – that is some evidence that the proposed common issue applies class-wide. The plaintiff's personal evidence about the existence of the alleged defect is not needed. Busy-body plaintiffs who are not directly affected by their proposed class action can be weeded out under s. 5(1)(e) or via a firm-handed application of the law of private interest standing.
>
> I note that the Court of Appeal in a recent decision, *Hodge v. Neinstein,*[33] had no difficulty with the one-step approach, making clear that "[a]t the certification stage, the factual evidence goes only to establishing whether the questions are common to all the class members."[34]

---

[30] *Kalra v. Mercedes Benz,* 2017 ONSC 3795 at paras. 41-47.

[31] See the discussion in *Dine v. Biomet, supra,* note 28, at paras. 15-19 and at note 9.

[32] *Pro-Sys, supra,* note 26, at para. 110.

[33] *Hodge v Neinstein,* 2017 ONCA 494.

[34] *Ibid.,* at para. 113, citing *Pro-Sys, supra,* note 26, at para. 110.

[52] However, the Divisional Court decided in 2017, just a few months after my decision in *Kalra,* that the two-step approach remains alive and well despite what was said by the Supreme Court in *ProSys*.

[53] In *Batten v Boehringer Ingelheim,*[35] the Divisional Court resuscitated the two-step test: (i) that the proposed common issue *actually exists*; and (ii) that the proposed issue can be answered in common across the entire class. Affirming the certification decision of the motion judge, the Divisional Court said this:

> [We] see no conflict between the common issues test as applied by the motions judge in the present case and the existing jurisprudence … There is no conflict between his approach and that in *Pro-Sys Consultants Ltd. v. Microsoft Corporation*, [2013] 3 S.C.R. 477. That case does not directly address a one stage versus a two stage inquiry. Rather, it emphasizes that "the factual evidence required at this stage goes only to establishing whether these questions are common to all the class members" (at para. 110). In my view, the motions judge applied the governing legal principles.[36]

[54] Respectfully, that is not what was said either by the Supreme Court in *Pro-Sys* or by the Court of Appeal in *Hodge v. Neinstein*, as set out above. There is obviously a conflict between *ProSys* and *Hodge*, on the one hand, and *Batten*, on the other. Do I follow the Supreme Court and Court of Appeal or am I bound by the more recent decision of the Divisional Court? Obviously the former. However, out of an abundance of caution, and given that an appeal herein is likely and the two-step, one-step issue will be clarified on appeal one way or the other, I will conduct my analysis of the PCIs using the two-step test.

[55] Section 5(1)(c) of the CPA requires that the claims or defences of the class members raise common issues. There is no dispute about the applicable law. For an issue to be common, it must be capable of being answered once for all class members. As noted in the leading class actions text:

> [I]f an issue can be resolved only by asking it of each class member, it is not a common issue …An issue is not "common" simply because the same question arises in connection with the claim of each class member, if that issue can only be resolved by inquiry into the circumstances of each individual's claim … The fact of a common cause of action asserted

---

[35] *Batten v Boehringer Ingelheim (Canada) Ltd.*, 2017 ONSC 6098 (Div. Ct.).

[36] *Ibid.* at paras. 14-15.

> by all class members does not in itself give rise to a common issue since the actual determination of liability for each class member may require individualized assessments.[37]

[56] The problem here, with almost all of the PCIs, is that there is no basis in fact for either the existence of the PCI or its overall commonality or both. Further, many of the PCI's, particularly those that ask about duty of care or breach of a standard of care, require so much in the way of individual inquiry that any commonality is overwhelmed by the need for individualized assessments.

[57] The plaintiffs point to s. 6 of the CPA and the statutory admonition that the court shall not refuse certification because "the relief claimed includes a claim for damages that would require individual assessment after determination of the common issues." I agree. Here, however, we don't get to any individual assessments that may be required "after determination of the common issues" because we don't have any certified common issues to determine.

[58] I will now consider each of the 30 PCIs in turn.

PCIs 1 to 6 – Negligence

[59] The first six PCIs ask whether the defendants owed a duty of care to those in the self-exclusion program, current or former employees and Players Passport Club members to take reasonable steps to establish, maintain and enforce appropriate security safeguards against a cyber-attack to limit the exposure of their personal information, and if so, whether the defendants breached the standard of care reasonably expected of them in the circumstances.

[60] The applicable duty of care and standard of care must first be established.

[61] In the *Saskatchewan Wheat Pool* decision,[38] the Supreme Court made clear that a statutory formulation of the applicable duty may afford "a specific, and useful, standard of reasonable conduct."[39] There can be no better statutory formulation of the applicable duty in a breach of privacy case, such as here, than what is set out in the federal privacy statute:

---

[37] Winkler, Perell, Kalajdzic and Warner, *The Law of Class Actions in Canada,* (2014) at 112-13, and case law cited therein.

[38] *R. v. Saskatchewan Wheat Pool,* [1983] 1 S.C.R. 205.

[39] *Ibid.,* at para. 42.

> 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.[40]

[62] In other words, the scope and content of the applicable duty and standard of care depends on the sensitivity of the personal information that has been collected. It is important to remember, as this court pointed out in *Broutzas*, that not all personal information is necessarily private or confidential:

> Generally speaking, there is no privacy in information in the public domain, and there is no reasonable expectation in contact information, which is in the public domain, being a private matter. Contact information is publicly available and is routinely and readily disclosed to strangers to confirm one's identification, age, or address.[41]

[63] Thus, applying federal statutory guidance, the less sensitive the information – such as simply one's name and mailing or email address, the lower the duty or standard of care; the more sensitive the information – credit card details, banking information or, say, medical records – the higher the duty and standard of care.

[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. Some of the personal information was private and confidential (banking details); much of it was relatively mundane (contact details only).

[65] There is no basis in fact to suggest that the question of whether the defendants breached any duty of care applicable to each class member can be answered in common across the entire class. Whether the defendants took reasonable steps to establish, maintain and enforce appropriate security safeguards (for the purposes of determining the nature and scope of the defendants' standard of care), will necessarily depend on the type and amount of personal information at issue.

[66] I agree with the defendants that on the evidence before the court the scope and content of the personal information that was stolen by the hacker varies so widely for each person that any assessment of the plaintiffs' claims quickly devolves into individual

---

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

[41] *Broutzas, supra,* note 8, at para. 153.

inquiries. Any common issues are completely overwhelmed by these individual investigations, such that commonality is not established and a class action cannot be justified as the preferable procedure.

[67] Turning to CPIs 1 to 6 specifically, there is no evidence, in affidavit form or otherwise, that any of the six duty or breach issues actually exist or can be answered in common across the possible sub-classes (self-excluder members, former or current employees or Players Passport Club members.) Each of CPIs 1 to 6 require highly individualized *ad hoc* assessments, a finding that fatally undermines any suggestion of commonality.

[68] CPIs 1 to 6 are not certified.

PCIs 7 to 15 – Breach of contract

[69] The next batch of PCIs relate to the breach of contract claim. In PCIs 7 to 13, the plaintiffs ask about enforceable contracts relating to former and current employees, Players Passport Club members who applied online (and arguably entered into online agreements about privacy expectations that were then breached by the defendants) and Players Passport Club members who applied at the Casino in person. PCIs 14 and 15 ask about the obligation of good faith in contractual performance.

[70] None of the breach of contract PCIs can be certified.

[71] PCIs 7 and 8 that ask about employees should be restricted, as noted above, to non-unionized employees. However, there is no evidence from any non-unionized employee of the actual terms or contents of any employment contracts (who exactly promised what to whom?) or that any such employment agreements were common across the class of all former and current, full and part-time, employees or that the breach of any such employment contracts relating to the non-unionized employees can be answered on a class-wide basis.

[72] PCIs 9 and 10 ask about Players Passport Club members who applied online but there is no evidence before the court from anyone who actually applied online. That is, there is no evidence that the PCIs 9 and 10 actually exist and/or can be answered on a class-wide basis.

[73] PCIs 11 and 12 ask about Players Passport Club members who applied not online but in person. But here again, there is no evidence from any such member about the terms or conditions of any actual contracts that may have been agreed to or that such terms and conditions were sufficiently similar that a class-wide determination would be possible.

[74] PCI 13 need not be answered because the answers to PCIs 8, 10 or 12 would not be "yes."

[75] PCI 14 and 15 asks about the defendants' duty to perform any such alleged agreements honestly and in good faith. There are two problems with this PCI. First, as I have already noted, no basis in fact has been presented for any such mutually binding agreements. Secondly, the duty of good faith in contractual performance requires that neither party lies to or misleads the other.[42] There is no evidence, in affidavit form or otherwise, that the defendants lied to or misled any of the class members or that any such issue could be decided on a class-wide basis without individualized assessments.

[76] PCIs 7 to 15 are not certified.

PCIs 16 to 18 and 23 – Breach of confidence and publicity given to private life

[77] Because neither of these two claims survived the s. 5(1)(a) analysis, the CPIs associated with breach of confidence and 'publicity given to private life' cannot be certified.

PCIs 19 to 22 – Intrusion upon seclusion

[78] PCIs 19 asks whether the defendants willfully or recklessly invaded the privacy or intruded upon the seclusion of the class members in its collection, use, retention and/or disclosure of the Personal Information in a manner that would be highly offensive to a reasonable person. PCIs 20 to 22 go on to posit three related questions.

[79] But here again, there is no evidence provided by way of affidavit or otherwise that any of the defendants invaded the class members' privacy, as opposed to the hacker. No evidence has been presented that any such invasion or intrusion was 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. And more importantly, no evidence that the determination of whether such invasion or intrusion was or would be highly offensive to a reasonable person could be decided class-wide on a common basis.

[80] In this case, individual inquiries would be required to determine if class members were in fact embarrassed or humiliated by the disclosure of the fact that they were, for example, patrons of Casino Rama. Even if one or more of the representative plaintiffs could prove that she was embarrassed or humiliated, and that her reaction was objectively reasonable in the circumstances, no methodology has been provided to show how the individual assessments could translate into class-wide determinations.

[81] PCIs 19 to 22 are not certified.

---

[42] *Bhasin v. Hrynew*, 2014 SCC 71 at para. 73.

PCIs 24 to 30 – Damages and administration

[82] Given that no PCIs have been certified that would establish liability in either tort or contract, there is no basis for the certification of any further PCIs dealing with damages. There is no basis for even a PCI that is limited to the availability of nominal damages for breach of contract – again, because no contract-based PCI has been certified.

[83] If there are no other certifiable issues in this proceeding, it follows that a common issue relating to punitive damages cannot be certified - the case law does not permit a "standalone" award of punitive damages.[43] In any event, there is no evidence advanced by anyone that the defendants engaged in "high-handed, malicious, arbitrary or highly reprehensible misconduct that departs to a marked degree from ordinary standards of decent behaviour."[44]

[84] An aggregate damages PCI should only be certified if liability has been established and there is some evidence that all or part of the defendant's monetary liability can reasonably be determined without proof by individual class members.[45] Here, liability cannot be established on a class-wide basis; nor have the plaintiffs provided any methodology by which damages can be calculated on a class-wide basis.

[85] PCI 25 asks about a gain-based remedy called disgorgement of profits. This PCI must have been added by mistake. This is obviously not a case about disgorgement of profits. In any event, there is no evidence that the defendants made any impugned profits that are or should be amenable to disgorgement.

[86] PCIs 28 to 30 that ask about further judicial directions, the payment of certain administrative costs, and the payment of pre-judgement and post-judgment interest would all have been left, even if I had found some certifiable PCIs, to the discretion of the trial judge. Absent any other certified PCIs, the questions set out in PCIs 24 to 30 have no context and are not certified.

Preferability

[87] It is "axiomatic" that if the common issues requirement is not satisfied, the preferable procedure requirement set out in s. 5(1)(d) of the CPA also cannot be

---

[43] *Batten v. Boehringer Ingelheim (Canada) Ltd.*, 2017 ONSC 53 at para. 206.

[44] *Whiten v. Pilot Insurance Co.*, 2002 SCC 18, at paras. 36, 69 and 94.

[45] *Kalra, supra,* note 30, at para. 67.

satisfied.[46] As explained above, there are no common issues in this case, and therefore the proposed class proceeding is not the preferable procedure for the resolution of the claims of the putative class members.

[88] Even though a class proceeding is not the preferable procedure, putative class members are not without recourse. Aside from the right to bring individual actions (for example, Mr. Champagne, if so inclined, could use the Small Claims Court to try to recover any additional credit monitoring costs that may have been incurred), claims for damages for breach of privacy can also be made under the federal privacy statue.[47]

Suitability of representative plaintiffs

[89] Given that no PCIs have been certified and there no basis for a class action, there is no need to discuss this last requirement.

Disposition

[90] The motion for certification is dismissed, primarily under s. 5(1)(c) of the CPA.

[91] If the parties cannot agree on costs, I would be pleased to receive brief written submissions – within 14 days from the defendants and within 14 days thereafter from the plaintiffs.

Justice Edward P. Belobaba

Date: May 7, 2019

---

[46] *Price v. H. Lundbeck A/S,* 2018 ONSC 4333 at para. 153.

[47] *PIPEDA, supra,* note 40, s. 16. The Federal Court's power to award damages under PIPEDA also includes the ability to award nominal damages where the plaintiff has not suffered actual pecuniary loss: *Blum v. Mortgage Architects Inc.*, 2015 FC 323 at para. 64.

Appendix

Proposed Common Issues

Negligence

1. Did the defendants, or any of them, owe a duty of care to Class Members enrolled in the Self-Exclusion Program to take reasonable steps to establish, maintain and enforce appropriate security safeguards against a cyber-attack to limit the exposure of their Personal Information?
2. If the answer to question 1 is yes, did the defendants, or any of them, breach the standard of care reasonably expected of them in the circumstances? If so, how?
3. Did the defendants, or any of them, owe a duty of care to Class Members currently or formerly employed at Casino Rama to take reasonable steps to establish, maintain and enforce appropriate security safeguards against a cyber-attack to limit the exposure of their Personal Information?
4. If the answer to question 3 is yes, did the defendants, or any of them, breach the standard of care reasonably expected of them in the circumstances? If so, how?
5. Did the defendants, or any of them, owe a duty of care to Class Members who were members of Casino Rama's Players Passport Club to take reasonable steps to establish, maintain and enforce appropriate security safeguards against a cyber-attack to limit the exposure of their Personal Information?
6. If the answer to question 5 is yes, did the defendants, or any of them, breach the standard of care reasonably expected of them in the circumstances? If so, how?

Breach of contract

7. Did Casino Rama Services enter into a contract with the Class Members currently or formerly employed at Casino Rama in respect of the collection, use, retention and/or disclosure of their Personal Information?
8. If the answer to question 7 is yes, did the contract between Casino Rama Services and the Class Members currently or formerly employed at Casino Rama contain express or implied terms that Casino Rama Services would utilize appropriate safeguards to protect these Class Members' Personal Information from unauthorized access and distribution?
9. Did Casino Rama Services enter into a contract with Class Members who applied online to join Casino Rama's Players Passport Club in respect of the collection, use, retention and/or disclosure of their Personal Information?

10. If the answer to question 9 is yes, did the contract between Casino Rama Services and the Class Members who applied online to join Casino Rama's Players Passport Club, contain express or implied terms that Casino Rama would utilize appropriate safeguards to protect these Class Members' Personal Information from unauthorized access and distribution?

11. Did Casino Rama Services enter into a contract with Class Members who applied at Casino Rama to be members of Casino Rama's Players Passport Club, in respect of the collection, use, retention and/or disclosure of their Personal Information?

12. If the answer to question 11 is yes, did the contract between Casino Rama Services and the Class Members who applied at Casino Rama to be members of Casino Rama's Players Passport Club contain express or implied terms that Casino Rama would utilize appropriate safeguards to protect these Class Members' Personal Information from unauthorized access and distribution?

13. If the answers to questions 8, 10, or 12 are yes, did the defendants, or any of them, breach these contracts? If so, how?

14. Did Casino Rama Services have a duty in the performance of its contractual obligations to act honestly and in good faith?

15. If the answer to question 14 is yes, did Casino Rama Services breach its duty in the performance of its contractual obligations to act honestly and in good faith? If so, to whom and how?

Breach of confidence

16. Did the collection, use and retention of the Class Members' Personal Information create an obligation of confidence in which the defendants were expected to protect and secure the Class Members' Personal Information?

17. Did storing Class Members' Personal Information without taking reasonable steps to establish, maintain and enforce appropriate security safeguards against a cyber-attack constitute an unauthorized use of the Personal Information?

18. Did one or more of the defendants breach the confidence of the Class Members? If so, how?

Privacy torts

19. Did Casino Rama Services, CHC Casinos or Penn National, willfully or recklessly invade the privacy of or intrude upon the seclusion of the Class Members in its collection, use, retention and/or disclosure of the Personal Information in a manner that would be highly offensive to a reasonable person?

20. If the answer to question 19 is yes, did Casino Rama Services, CHC Casinos or Penn National commit the tort of intrusion upon seclusion? If yes, why? (sic).

21. Would the posting online of the Personal Information of those Class Members' whose Personal Information was contained in one of the two "data dumps" be highly offensive to a reasonable person of ordinary sensibilities?

22. Was the Personal Information of those Class Members' whose Personal Information was contained in one of the two "data dumps" of legitimate concern to the public?

23. If the answers to questions 21 and 22 are yes, did one or more of the defendants commit the tort of publicity given to private life?

Damages & administration

24. Are the defendants, or any of them, liable for damages to the Class Members for negligence, breach of contract, breach of confidence, intrusion upon seclusion and/or publicity given to private life?

25. Is this an appropriate case for the defendants, or any of them, to disgorge profits?

26. Are the defendants, or any of them, liable for punitive damages?

27. If the answer to question 24 is yes, can the court assess damages in the aggregate, in whole or in part, for the Class Members for negligence, breach of contract, intrusion upon seclusion and/or publicity given to private life? If so, what is the amount of the aggregate damage assessment(s) and who should pay it to the Class?

28. If the answer to question 24 is yes, and if the court considers that the participation of individual Class Members is required to determine individual issues:

    (i) Are directions necessary?

    (ii) Should any special procedural steps be authorized?

    (iii) Should any special rules relating to admission of evidence and means of proof be made?

    (iv) What directions, procedural steps or evidentiary rules ought to be given or authorized?

29. Should the defendants, or any of them, pay the costs of administering and distributing any amounts awarded under ss. 24 and 25 of the *CPA*? If so, who should pay what costs, in what amount and to whom?

30. Should the defendants, or any of them, pay pre-judgment and post-judgment interest? If so, at what annual interest rate? Should the interest be simple or compound?

***