Federal Court Cour fédérale

Date: 20240606

Docket: T-226-13

Citation: 2024 FC 851

Ottawa, Ontario, June 6, 2024

PRESENT: Associate Chief Justice Gagné

PROPOSED CLASS PROCEEDING

BETWEEN:

JOHN MARK JACQUES, GORDON ALBERT MEHEW, AND CRAIG ROBAR

Plaintiffs

and

HIS MAJESTY THE KING

Defendant

ORDER AND REASONS

I. Overview

[1] This is a motion for certification of a proposed class action. The Plaintiffs allege that an employee (or employees) of the Department of Human Resources and Skills Development

Canada, now Employment and Social Development Canada (Employment Canada) acted negligently and breached the confidence of applicants for Canada Pension Plan Disability Benefits when they lost a USB key containing their personal information.

[2] The facts at the origin of this claim occurred in November 2012 and the Statement of Claim was filed in January 2013, a few weeks after similar claims were brought in files T-132-13 (the *Condon* file) and T-166-13.

[3] Counsel for the parties in all three related files agreed to consolidate files T-132-13 and T-166-13 and to use the *Condon* file as the lead file, while keeping the present file in abeyance until final disposition of the *Condon* file.

[4] The Condon file was certified and a judgment of this Court approved the settlement, effective July 17, 2018.

[5] Besides arguing that the test for certification is not met in this file, the Defendant now states that the claims of most of the class members are barred by lapsed limitation periods.

II. Facts

A. *The loss of the USB key*

[6] In November 2012, an unnamed employee of Employment Canada provided a lawyer from the Department of Justice (DOJ) with an unencrypted USB key containing the personal information of 5,045 people who were appealing the denial of their disability benefits.

[7] The next day, the USB key was lost. A search was made of the employee's office, home and the taxi the employee took home that day but no one has been able to locate the USB key to date.

[8] In December 2012, the Plaintiffs and presumably all the class members received a letter from Employment Canada notifying them that a USB key with their personal information had been misplaced. The letter read in part:

> … I regret to inform you that an electronic storage device, also known as a USB key, which contained some of your personal information, was misplaced by an employee. It contained the following types of information: Social Insurance Number (SIN); surname; primary and, if applicable, secondary medical condition; birthdate; presence of other payers (e.g., workers' compensation); level of education; occupation type; and, Service Canada processing centre.

[9] The members of the class are defined as:

> All persons whose personal information was contained in an electronic storage device, also known as a USB key, in the control of Human Resources and Skills Development Canada or the Department of Justice, which was lost or disclosed to others in or about November, 2012.

[10] The Defendant has since confirmed that the USB key contained the following information:

> Last name; Date of birth; Social Insurance Number ("SIN"); Level of education and occupation type; Service Canada processing centre; Generic medical condition by way of coding flowing from the International Classification of Diseases, and; Confirmation of other payers, such as workers' compensation programs.

[11] In December 2012, Employment Canada informed the Office of the Privacy Commissioner of Canada (Privacy Commissioner) of the breach. The loss of this data was publicly disclosed in a press release issued on January 11, 2013 by Employment Canada, which stated that:

> In late 2012, the department of Human Resources and Skills Development Canada (HRSDC) informed the Office of the Privacy Commissioner of the loss of a USB key, which contained the personal information of over 5,000 Canadians.

[12] Later that month, members of the proposed class received a second letter from Employment Canada, offering to have a notation placed on the recipient's credit file (a credit flag) to warn creditors to confirm the recipient's identity before extending credit. In October 2014, the Privacy Commissioner published an announcement of the findings of its investigation, entitled "Lost USB key from Employment and Social Development Canada reinforces lessons learned."

[13] The Privacy Commissioner wrote the following:

> That same month, a USB key containing the personal information of 5,045 Canada Pension Plan Disability appellants disappeared from a desk in an ESDC office. As with the hard drive, the USB key was neither password-protected nor encrypted, nor was it ever

> found. The missing personal information included each individual's SIN, date of birth, surname, medical conditions, date of birth, education level, type of occupation and whether other payments were being received, such as worker's compensation. In the wrong hands, such information could lead to identity theft or fraud.

[14] The Privacy Commissioner found that the DOJ, whose lawyer had custody of the USB key when it went missing, "failed to translate its security and privacy policies into meaningful business practices." In other words, the employee, a lawyer with custody of the USB key, failed to adhere to, or disregarded, established security and privacy policies.

[15] The facts in this case are similar to those in the *Condon* file in which a portable hard drive containing student loan applications had been lost.

[16] The *Condon* file came to light at the same time as the loss of the USB key in this matter. According to a Special Report to Parliament by the Privacy Commissioner, dated March 25, 2014:

> …[O]n November 5, 2012, an employee of the CSLP Unit went to retrieve an external hard drive from a filing cabinet and noticed that it was missing. … According to ESDC's representations, the hard drive was stored in a lockable filing cabinet located in that employee's cubicle, in an envelope, hidden under suspended files. … It was not password protected, nor was the information contained on it encrypted. The serial number of the hard drive remains unknown. … Following a comprehensive review of the files and folders on the Department's network that were identified for the migration project, ESDC informed our Office that the following data files were compromised by the loss of the external hard drive, each of which is described in more detail below:
>
> > • Files pertaining to client satisfaction surveys;• Files containing investigation reports;• Files containing CSLP financial, business plan and

> Human Resources information;• Files containing Business Continuity Planning information.
>
> Notwithstanding the above, as the hard drive is missing, ESDC submits that there is no way to conclusively identify what information was in fact backed up to the hard drive.

[17] Just as with its report on the loss of the USB key, the Privacy Commissioner concluded, with respect to the *Condon* file, that Employment Canada had failed to translate its own privacy and security policies into meaningful business practices.

[18] In the wake of *Condon*, the Privacy Commissioner made several recommendations, which Employment Canada accepted, including but not limited to:

> • We recommended that ESDC revisit its physical security control practices to ensure that regular monitoring and inspections are incorporated into its security program. This will help to ensure that personal information is stored in approved cabinets when employees are away from their desks for any length of time; that cabinets are locked accordingly; that keys for cabinets are properly safeguarded; and that attractive or valuable assets (i.e. external hard drives, laptops, etc.) containing personal information are properly safeguarded.
>
> • We recommended that portable storage devices only be used as a last resort to store or transfer personal information, and only if it is demonstrably necessary to fulfill a specific and documented purpose. All sensitive or personal information stored on portable devices must be protected by strong technological safeguards, including encryption.
>
> • We recommended that ESDC's training and awareness program include a particular focus on … Strategies to ensure that all employees understand their roles and responsibilities for the management of personal information … The requirements for physical security outlined in ESDC's own "Departmental Security Policy and Procedures Manual" … The requirements for safeguarding personal information … [and] The consequences of not adhering to Departmental security and privacy standards.

[19] The Plaintiffs are representative class members who have been informed by Employment Canada that their information was included on the lost USB key.

B. *The investigation*

[20] The Defendant has provided evidence that the two departments responsible for the employees undertook formal administrative investigations into allegations of mishandling of information. Their affiant states that the internal investigations concluded that Employment Canada and DOJ's employees did not treat classified information consistently with departmental policy, but that there was no evidence that the USB key was stolen, accessed for fraudulent purposes, or taken outside the office.

III. Test for Certification

[21] Rule 334.16(1) of the *Federal Courts Rules*, SOR/98-106 [the Rules] sets out the conditions for certification of a class action. It prescribes that a class action shall be certified if: (a) the pleadings disclose a reasonable cause of action; (b) there is an identifiable class of two or more persons; (c) the claims raise common questions of law or fact; (d) a class proceeding is the preferable procedure for the just and efficient resolution of those common questions; and (e) there is an appropriate representative plaintiff.

[22] All but the last of these conditions are at issue in this motion.

[23] The test applied under subsection (a), whether the pleadings disclose a reasonable cause of action, is the same as that on a motion to strike – "whether it is plain and obvious that the pleading discloses no reasonable cause of action" (*Sweet v Canada*, 2022 FC 1228, at para 75). This analysis is not to be based on the evidence, but rather on the assumption that the facts, as pleaded, are true.

[24] The threshold for meeting the other requirements for certification (subsections (b) to (e)) requires the Plaintiffs to adduce evidence that shows "some basis in fact" in support of the certification order. That threshold does not require the party seeking certification to establish the certification requirements on a balance of probabilities. It does not require the Court to resolve conflicting facts and evidence but rather reflects the fact that, at the certification stage, the Court is ill-equipped to resolve conflicts in the evidence or to engage in finely calibrated assessments of evidentiary weight (*Pro-Sys Consultants Ltd v Microsoft Corporation*, 2013 SCC 57, at paras 101-102). However, the standard for assessing evidence at that stage does not involve such a superficial level of analysis into its sufficiency that it would amount to nothing more than symbolic scrutiny (*Pro-Sys*, at para 103).

[25] The certification test is conjunctive. If a plaintiff fails to meet any of the five listed criteria, the certification motion must fail.

[26] Recently in *Jensen v Samsung Electronics Co Ltd*, 2023 FCA 89 [*Jensen FCA*], the Federal Court of Appeal emphasized that the certification stage remains an important gate-keeping mechanism which must operate as a meaningful screening device and which shall not be

treated as a mere formality. The Court agreed with the approach set out by Justice Denis Gascon of this Court (*Jensen v Samsung Electronics Co Ltd*, 2021 FC 1185) [*Jensen FC*]:

> [292] I do not dispute that the class actions are a specific procedural vehicle for litigants and that a certification motion is not the place to focus on the substance and merits of a contemplated class action. However, the certification stage nonetheless remains an important gate-keeping mechanism which must operate as a "meaningful screening device" and which shall not be treated as a "mere formality" (*Desjardins*, at para 74; *Oratoire*, at para 62; *Pro-Sys*, at para 103). Contrary to what the Plaintiffs appeared to suggest, for a court to conduct a rigorous review of the material facts and the evidence put forward by a plaintiff on a certification motion does not amount to delving into the merits of the case. As the [Supreme Court of Canada] frequently stated, it is rather part of the courts' expected role and duty to do more than a rubber-stamping and symbolic review of proposed class actions at the certification stage, and to be satisfied that the certification requirements are effectively met.

IV. Issues

[27] This certification motion raises the following issues:

A. *Do the pleadings disclose a reasonable cause of action?*

B. *Is there an identifiable class of two or more persons or are the claims of most of the class members barred by lapsed limitation periods?*

C. *Does the claim raise common questions of law and fact?*

D. *Is a class proceeding the preferable procedure for the just and efficient resolution of the common questions?*

V. Analysis

A. *Do the pleadings disclose a reasonable cause of action?*

[28] The first requirement for certification is whether the pleadings disclose a reasonable cause of action (Rule 334.16(1)(a) of the Rules). The test applied to this requirement is the same as on a motion to strike, i.e. whether it is plain and obvious that the pleadings disclose no reasonable cause of action. This analysis is to be conducted on the assumption that the facts as pleaded are true, not on evidence submitted by the parties (*Condon v Canada*, 2015 FCA 159 at paras 11-13) [*Condon FCA*].

[29] The Defendant does not dispute that the pleadings disclose a reasonable cause of action in negligence (although he argues there is no basis in fact for harm or damages suffered by the Plaintiffs/class members; we will come back to this later). However, the Defendant strongly disputes that the pleadings disclose a cause of action in breach of confidentiality.

[30] Breach of confidence is an intentional tort, which requires the plaintiff to: (a) communicate confidential information, (b) in confidence, and requires the defendant to (c) misuse the information, (d) intentionally, and (e) to the detriment of the plaintiff (*Lac Minerals Ltd v International Corona Resources Ltd*, 1989 CanLII 34 (SCC) at p 576).

[31] The parties agree on the definition of the tort. However, they disagree on what constitutes "intention". The Plaintiffs argue it is the misuse of the confidential information that needs to be

intentional, whereas the Defendant argues that the confidee needs to use the confidential information with the intention to cause harm or detriment to the confider.

[32] The Plaintiffs plead that the information (especially the social insurance numbers and the medical information) was confidential and communicated in confidence. They plead that the loading of the information onto an unencrypted USB key and removing it from the offices (rather than storing it in a security-approved container such as a locked cabinet) constituted intentional misuse, as the employees knew they were contravening the departmental manual and its policies and practices for Protected B information. For the Plaintiffs, the claim of breach of confidence is pleaded with particularity and material facts are set out. They rely on the recent decision of the Supreme Court of British Columbia in *Lam v Flo Health*, 2024 BCSC 391, and on the fact that the same claim was certified in the *Condon* file. As such, it is not plain and obvious that the claim cannot succeed.

[33] In *Sweet*, Justice Richard Southcott had to deal with a similar debate between the parties. The plaintiffs' online government accounts were hacked as a result of alleged operational failures by the defendant to properly secure the portals providing access to these accounts. Amongst others, the plaintiffs were advancing a cause of action based on the tort of breach of confidence. As in the present case, the defendant had submitted that its failure to prevent the cyber attacks does not constitute misuse within the meaning of this tort.

[34] Although Justice Southcott recognized there was jurisprudential support for the defendant's position, he nevertheless found that it was not plain and obvious that the plaintiffs'

cause of action in breach of confidence was doomed to fail, essentially because a similar cause of action was certified in *Condon* and in T-1931-13 (the *Doe* file):

> [121] In the *Del Giudice* hacking case described earlier in these Reasons, the Ontario Superior Court of Justice found no basis for a breach of confidence claim based on the material facts pleaded, both because most of the information was not confidential and because, in the view of the Court, the defendants did not make an unauthorized use of the information such as would constitute its misuse (at para 197). Similarly, in *Kaplan v Casino Rama Services Inc*, 2019 ONSC 2025 [*Kaplan*], the Ontario Superior Court of Justice reasoned that, unless the word "misuse" was distorted out of all shape and meaning, the defendants' failure to prevent the cyberattack at issue in that case was not a misuse of confidential information within the meaning of the breach of confidence tort (at para 31).
>
> [122] In response to this argument, the Plaintiff relies on *Condon FCA* and *John Doe FCA*, both of which allowed the certification of breach of confidence claims in circumstances where the Government failed to adequately safeguard confidential information. In *Tucci BCCA*, upon which I have previously relied in these Reasons, the Court of Appeal for British Columbia considered *Condon FCA*, as well as the Federal Court decision in *John Doe*, as authorities identified by the plaintiffs in which breach of confidence claims had been allowed to proceed in circumstances similar to the online data breach it was considering. The Court of Appeal noted that neither of these authorities of the Federal Courts specifically addressed the issue of whether the tort of breach of confidence requires intentional misuse of confidential information (at para 112). While the certification of proceedings in those two cases appeared inconsistent with a view that misuse must be intentional, the Court of Appeal for British Columbia nevertheless concluded that breach of confidence is an intentional tort (at paras 112-113).
>
> [123] As such, *Tucci BCCA* represents another authority supporting the Defendant's position that the tort of breach of confidence does not apply to the circumstances of the case at hand. Nevertheless, I am conscious of the principle adopted by Justice Martineau in *Arsenault v Canada*, 2008 FC 299 [*Arsenault*] at para 27, that, in order to meet the test on a motion to strike (which is the same test that applies under Rule 334.16(1)(a)), there must be a decided case directly on point, from the same jurisdiction, demonstrating that the very issue has been squarely dealt with and rejected.

> [124] Consistent with the observation in *Tucci BCCA*, neither *Condon FCA* nor *John Doe FCA* dealt expressly with the issue presently before the Court, i.e. whether the requirement of misuse in the tort of breach of confidence that can be met in the absence of intention on the part of the alleged tortfeasor. Indeed, as the Defendant submits, the case at hand is somewhat distinguishable even from *Condon FCA* and *John Doe FCA*, as neither of those cases involved a third party actor. However, I understand the Plaintiff's reliance on these authorities, as both involved the Government failing in some manner to properly safeguard confidential information. Given that level of similarity, the fact that certification was granted in both cases, and the fact that they represent decisions of the Federal Court of Appeal, and taking into account the principle in *Arsenault*, I am unable to conclude that the Plaintiff's cause of action in breach of confidence is doomed to fail.

[35] Besides the fact that in *Condon FCA* and in *Canada v John Doe*, 2016 FCA 191 [*John Doe FCA*], the issue before the Court was not as articulated by the parties in *Sweet* — and in the case at bar, there is now such a "decided case directly on point, from the same jurisdiction, demonstrating that the very issue has been squarely dealt with and rejected" (*Sweet*, at para 123).

[36] After the *Doe* case was finally certified by this Court in *John Doe v Canada*, 2022 FC 587, the Court was seized with a motion for summary judgment brought by the plaintiffs who asserted that all common issues should be ruled in their favour and that there were no genuine issues for trial. Justice Catherine Kane granted the motion in part but dismissed the claim based on the tort of breach of confidence (*John Doe v Canada*, 2023 FC 1636) [*Doe Summary Judgment*].

[37] In that case, the plaintiffs' claims arose from Health Canada's mass mail-out of over 41,000 letters to participants in the Marihuana Medical Access Program in November 2013. The

letters were sent in an envelope with a see-through window, which displayed the sender's return address as "Marihuana Medical Access Program" and the full name and address of the recipient. The plaintiffs alleged that the mass mail-out "outed" their participation in the program, disclosed their confidential information, and violated their right to privacy.

[38] The common issues on the breach of confidence were the following:

- Did the Class Members communicate the Personal Information to Health Canada?
- If yes, did Health Canada misuse the Personal Information in its collection, use, retention or disclosure of the Personal Information?
- If yes, was such misuse of the Personal Information to the detriment of the Class Members?
- If yes, did Health Canada breach the confidence of the Class Members in its collection, retention or disclosure of the Personal Information?

[39] Justice Kane answered the first two questions in the affirmative and the third and fourth questions in the negative.

[40] The plaintiffs had argued that common law should continue to evolve to recognize the tort of breach of confidence without requiring proof of detriment and to recognize that breach of confidence should be actionable *per se*.

[41] Justice Kane rejected that argument and found that applying the test in the way the plaintiffs were suggesting "would result in a new tort for privacy claims with lower thresholds

than the tort of intrusion upon seclusion and the statutory torts that exist in some provinces" (*Doe Summary Judgment*, at para 148).

[42] After having found that the class members communicated personal information to Health Canada, who had misused it, Justice Kane stated that misuse on its own did not establish the tort. The *Lac Minerals* test, and subsequent jurisprudence applying the test, requires that the misuse be to the detriment of the confider and that the misuse, and resulting breach of confidence be intentional (see for example *Tucci v Peoples Trust Company*, 2020 BCCA 246 and *Lysko v Braley et al*, 2006 CanLII 11846 (ON CA)).

[43] Even if the misuse of the class members' information was not accidental — Health Canada had approved the see-through envelopes — Justice Kane found that the misuse was not intentional. The evidence before her showed that Health Canada did not intend to misuse confidential information and did not intend to betray the confidence of class members or to cause them any harm.

[44] The Plaintiffs argue that the Supreme Court of British Columbia in *Lam* issued a few months after this Court's decision in *Doe Summary Judgment* clearly contradicts its finding. The Plaintiffs assert that if there is conflicting jurisprudence, it is not plain and obvious the claim is doomed to fail.

[45] *Lam* was an application for certification of a proposed class action under the British Columbia *Class Proceeding Act*, RSBC 1996, c. 50. The plaintiff alleged that the defendant

intentionally violated the privacy of people who used the Flo Health & Period Tracker application to track their reproductive cycles. The proposed class representative says that she and others used the App and entered highly sensitive personal health information relating to their reproductive system, relying on the defendant's assurances that the information would be kept private. In fact, the defendant had sold the personal information of the App users to third parties like Facebook for advertisement purpose.

[46] Having enunciated the test set out by the Supreme Court of Canada in *Lac Minerals*, Justice Blake states that the tort of breach of confidence "is well-defined as an intentional tort" (*Lam*, at para 71). The critical issue being whether the confidential information was misused, she found that this element of the tort was met since Flo misused "the information by failing to adhere to the terms of their privacy policies, as well as PIPEDA and industry standards, and that it did so for its own financial gain, to the detriment of the class members" (*Lam*, at paras 72, 73, 76).

[47] In other words, the misuse in *Lam* was the intentional disclosure of the confidential information to third parties (*Lam*, at para 76).

[48] In the case before me, the uncontradicted evidence shows that employees of Employment Canada (business and legal) were working on appeals pending before the former tribunal when the USB key was lost. The key was used to store and share the information of the appellants that were being triaged by counsel for the purpose of appeals.

[49] The Plaintiffs focus on the different terms used to explain what occurred: the USB key disappeared or was lost (language used by the Privacy Commissioner) or it was misplaced (used in the December letter from Employment Canada to the class members).

[50] Yet, there is no evidence that the USB key was stolen and contrary to what the Plaintiffs assert, the reference made by the Privacy Commissioner to its disappearance does not infer that it was stolen. In my view, it is a poor use of the word as it is well know that, unless David Copperfield is involved, a USB key does not simply disappear. In fact, the use of words does not change the reality; nobody knows what really occurred to the USB key.

[51] More importantly, the Plaintiffs do not plead that their confidential information was disclosed or accessed by any third party as a result of the loss of the USB key.

[52] Relying on *Lam*, the Plaintiffs are asking the Court to jump a few steps: they basically say that simply because the USB key was used in a non-permitted way (it should have been encrypted and stored in a locked cabinet and it was not), the Court should find that there was intentional disclosure, and that that disclosure caused detriment to the class members. In other words, they want the Court to find that misuse equates intention and intention equates detriment.

[53] With respect, the Court cannot overlook those missing elements of the tort.

[54] For these reasons, I am of the view that, on the assumption that the facts pleaded are true, the Plaintiffs have not made a cause of action in breach of confidence.

B. *Is there is an identifiable class of two or more persons or are the claims of most of the class members barred by lapsed limitation periods?*

[55] Although the Defendant states that the limitation period has an impact on several elements of the test for certification, he argues the Plaintiffs clearly fail to meet the requirement under Rule 334.16 because the claims of the putative class members are statute barred by limitation periods.

[56] The Plaintiffs were first relying on a Nova Scotia Supreme Court decision for the proposition that the expiration of a limitation period is a defence that must be pled in a statement of defence. Since the defendants chose not to file a statement of defence before certification, limitation was not an issue at certification (*MacQueen v Sydney Steel Corporation*, 2011 NSSC 484 (CanLII) at para 73).

[57] At the hearing, the Plaintiffs sought leave to file the affidavit of Luciana Brasil to document communications between counsel and the Court leading up to the parties' request to suspend this proceeding pending the outcome in the *Condon* file. The Court granted leave and heard the parties' arguments on the issue.

[58] The *Crown Liability and Proceedings Act*, RSC 1985, c C-50 provides that where a cause of action arises "otherwise than in a province," proceedings "shall be taken within six years after the cause of action arose" (section 32). Identical language is used in subsection 39(2) of the *Federal Courts Act*, RSC 1985, c F-7.

[59] The Defendant takes the position that the putative class' claims expired in **December 2018**, six years after the class members were informed of the incident in December 2012. The Plaintiffs, on the other hand, are of the opinion that it will expire on September 23, 2024. The Plaintiffs rationale is as follows:

- The parties agree that the applicable limitation period to bring the action is 6 years.
- Assuming all class members discovered their claim based on a December 19, 2012 letter, which is denied, the class period began running on December 20, 2012.
- The parties agreed to a suspension on April 14, 2013. This suspension was ultimately extended until the full resolution of the *Condon* file.
- The *Condon* file was settled and the settlement agreement was approved on May 18, 2018. The matter would have been fully resolved after 60 days, which brings the end of the suspension to July 17, 2018.
- Finally, there was a 6 month (March 13, 2020 until September 13, 2020) where the limitation period was suspended due to COVID-19.
- A period of six years is made up of 2190 days.
- Assuming the time began running on December 20, 2012, which is denied, 116 days elapsed before the agreement to suspend the case.
- On the plaintiff's view, the limitation period began running again on July 18, 2018, when the settlement approval order in the *Condon* file became final, and ran until it was suspended again due to Covid on March 13, 2020. The period between July 18, 2018 and March 13, 2020 is an additional 605 days.
- At this point, there were 1469 days left in the limitation period.
- The class period began running again on September 15, 2020, when the Covid suspension ended. 1469 days after September 15, 2020 is **September 23, 2024**.

[60] Under this Court's class action regime, time is only tolled once the class is certified. In the absence of a provision suspending the limitation period for putative class members, they must file individual claims, or otherwise preserve their right by way of an agreement between the parties to toll the limitation period pending certification.

[61] A discussion paper of the *Federal Courts Rules Committee* illustrates the issue. The committee chose not to adopt a provision suspending the limitation period pending certification of a class action (Federal Court of Canada Rules Committee, Class Proceedings in the Federal Court of Canada: A Discussion Paper (June 9, 2000), XVII LIMITATION PERIODS, at pp 93-96, Defendant's Motion Record, tab 6). The committee stated:

> It would be helpful for plaintiffs to have such a provision regarding the suspension of limitation periods. However, the constraints on the jurisdiction of the Committee prevent the class proceedings rule from addressing this question. Limitation periods clearly deal with matters of substance. Without such a provision, members of the class may have to file a statement of claim to preserve their rights pending the determination of whether the class will be certified. The need to file a statement of claim in such circumstances, or to seek an agreement from the defendant that the limitation period will not be raised as a defence, may be a burden, but it is not an onerous one. In any event, such a requirement on the part of members of the class does not otherwise impair the viability of the class proceedings rule. Notices sent to class members, before the disposition of the proceedings on the merits, may need to warn members of the class that any relevant limitation periods continue to apply.

[62] This Court has found that a class proceeding could not be used to resurrect the rights of individuals that were statute barred for limitations through their participation in a class action (*Tihomirovs v Canada (Minister of Citizenship and Immigration)*, 2006 FC 197 at para 92; *Vézina v Canada (Defence)*, 2011 FC 79, at para 43).

[63] In other words, unlike provincial class proceedings regimes, this Court's regime requires a tolling agreement or certification to toll the limitation period.

[64] The Defendant takes the position that, although the Plaintiffs filed their statement of claim on January 31, 2013, the parties never agreed to toll the running of the limitation period against the putative class, and the Defendant never agreed to waive its right to raise limitations.

[65] On April 15, 2013, at a case management conference, the parties agreed to keep this file in abeyance while the *Condon* litigation proceeded. However, limitations are substantive rights. The Court could only suspend procedural court filing deadlines for the representative plaintiffs under the Federal Courts Rules.

[66] The Plaintiffs refer to the decision of this Court in *McCrea v Canada (Attorney General)*, 2015 FC 592, to assert that limitation periods do not need to be determined at certification. However, *McCrea* dealt with a situation in which some of the class' claims had expired whereas some others had not. In such a situation, Justice Kane found that the limitation period did not prevent certification. The present case is distinguishable because the claim was discoverable at the same time for all plaintiffs when they received notice from Employment Canada of the data loss. As such, the limitation period question is determinative for the entire class (except for the three Plaintiffs). Given the gatekeeping mechanism of the certification motion, it would not be in the interests of judicial economy to certify a class action that was completely statute barred for all proposed plaintiffs.

[67] The question is therefore whether there was a tolling agreement between the parties, or whether the Defendant agreed to waive limitations.

[68] The Plaintiffs first assert that the Defendant agreed to suspend the limitation period when they agreed to the suspension of the case.

[69] Yet, the Plaintiffs could not point to any explicit or implicit agreement, may it be oral or in writing, and the Defendant states it never agreed to waive its right to raise limitations.

[70] In her affidavit, Ms. Brasil states that the Plaintiffs first received notice of the Defendant relying on the statute of limitations in February 2024, when they were served the Defendant's memorandum of fact and law. However, correspondence filed in support of her affidavit clearly shows that the issue was discussed between the parties in June 2023. Counsel for the Plaintiffs asked counsel for the Defendant whether the latter intended to rely on the limitation period at certification. This also confirms that no agreement had previously been reached between the parties to toll the limitation period.

[71] The Plaintiffs also argue that the Defendant is estopped from arguing the limitation period. Promissory estoppel is an equitable defence which requires a party to establish that:

> (1) The other party has, by words or conduct, made a promise or assurance which was intended to affect their legal relationship and to be acted on; and
>
> (2) The party arguing promissory estoppel relied on the promise or assurance by taking some action or in some way changing its position.

> (*Maracle v Travellers Indemnity Co of Canada*, 1991 CanLII 58(SCC), [1991] 2 SCR 50 at p 57).

[72] The Supreme Court of Canada's most recent guidance is that the equitable defence of promissory estoppel requires that (1) the parties be in a *legal relationship* at the time of the promise or assurance; (2) the promise or assurance be *intended* to affect that relationship and to be acted on; and (3) the other party in fact *relied* on the promise or assurance (*Trial Lawyers Association of British Columbia v Royal & Sun Alliance Insurance Company of Canada*, 2021 SCC 47 at para 15).

[73] There is no dispute in the jurisprudence that the promise must be "clear and unequivocal" or "unambiguous" (*Trial Lawyers Association of British Columbia v Royal & Sun Alliance Insurance Company of Canada*, 2021 SCC 47 at paras 46, 59).

[74] The success of the Plaintiffs' defence of promissory estoppel therefore largely hinges on whether they provided clear and unequivocal evidence that the Defendant intended to promise to waive the limitation period.

[75] In my view, the Defendant's conduct does not clearly indicate an intent to waive the limitation period. In addition, the Plaintiffs' conduct — seeking information on the Defendant's position on the issue — shows that they did not interpret the Defendant's conduct as that of a party who had waived a substantive right. Therefore, they could not have been relying upon such a promise.

[76] This Court has no inherent jurisdiction to permit a proceeding that is entirely out of time to be commenced (*Tacan v Canada*, 2005 FC 385, [2005] FCJ No 497, at paras 87, 88; *Nicholson v Canada*, [2000] 3 FC 225, FCJ No 211, at paras 38 to 41). Absent an express statutory grant of discretion, a limitation period cannot be waived or extended by the Court.

[77] In the absence of a tolling agreement waiving the Defendant's substantive statutory rights, I am of the view that the limitation period was not tolled and the putative class' claims are statute-barred.

[78] In my view, this conclusion is dispositive of the Plaintiffs' motion. However, in case I am mistaken on the limitation issue, I will discuss a few additional reasons why I am of the view that the Plaintiffs do not meet the test for certification.

C. *Does the claim raise common questions of law and fact?*

[79] The Plaintiffs seek certification of the following common issues:

> **Negligence**
>
> 1. Did the Defendant owe class members a duty of care in its collection, retention, and/or disclosure of the Personal Information?
>
> 2. If the answer to #1 is yes, did the Defendant breach the standard of care in its collection, retention, loss, and/or disclosure of the Personal Information? If yes, why?
>
> **Breach of confidence**
>
> 3. Did the class members communicate the Personal Information to the Defendant in confidence?

4. Did the Defendant misuse the Personal Information in its collection, retention, loss, and/or disclosure of the Personal Information, and was that misuse to the detriment of the class members?

5. If the answers to #3 and #4 are yes, did the Defendant breach the confidence of the class members and, if so, how?

Vicarious Liability

6. Is the Defendant vicariously liable or otherwise responsible for the acts and/or omissions of its officers, directors, employees, agents and representatives while in possession of the Personal Information?

Damages

7. If one or more of common issues are answered in the affirmative, should the Defendant pay compensable damages that were caused by the Defendant's:

a. Negligence?

b. Breach of confidence?

8. Can the class members' damages be assessed in the aggregate pursuant to Rule 334.28(1) of the Federal Courts Rules? If so, in what amount?

9. Are the class members entitled to pre and post-judgment interest pursuant to the *Crown Liability and Proceeding Act*, RSC 1985, c C-50? If so, at what rate?

[80] As indicated above, the threshold for meeting the other requirements for certification is the establishment of "some basis in fact" to support the certification order.

[81] That test has a dual component. First the putative class members must have a claim, or at the very least, some minimal evidence supporting the existence of a claim. Second, there must be some evidence that the common issues are such that their resolution is necessary to the resolution

of each class member's claim (*Jensen FCA*, at para 78; *Hollick v Toronto (City)*, 2001 SCC 68, para 25).

[82] The two-step test requires the court to review the evidence adduced in support of the motion. In *Jensen FC*, this Court describes the task as a "rigorous review" (at para 292) and noted that the standard requires some basis in fact, not proof of fact to the civil standard. A review of the evidence to satisfy the existence of a claim at this stage of the analysis is different than weighing the merits of the claim. As this Court stated in *Jensen FC*, "[t]here is a fundamental difference between weighing the merits of the claim (which the courts cannot do at certification) and determining whether some minimal evidence exists to support the existence of the claim" (i.e., the two-step test) (at para 212; *Jensen FCA* at para 79).

[83] The Defendant concedes that issues 1 and 2 could be determined in common; however, he asserts issues 4 and 5 have no basis in fact and issues 7 and 8 (Damages) cannot be determined in common and have no basis in fact.

(1) Issues 4 and 5 Breach of confidentiality

[84] The Plaintiffs did not provide detailed arguments on these proposed common questions or on what would meet the "some basis in fact" test specifically regarding the breach of confidence claim.

[85] In my view, there is no basis in fact to ground the proposed common issues 4 and 5. The Plaintiffs have no basis in fact to establish that Employment Canada intended to betray or harm

the Plaintiffs or that it caused them detriment. None of the representative plaintiffs' affidavits shed any light on intentionality. Nor do they provide any material facts or particulars relating to their detriment. To the contrary, they depose that to the best of their knowledge, their information has not been accessed by third parties.

(2) Issues 7 and 8 Damages

(a) *Common damages in negligence*

[86] At the hearing, counsel for the Plaintiffs described the evidence filed in detail. The question is whether there is some basis in fact that there are compensable damages sufficient to support the negligence claim and some evidence that the resolution of the common issues is necessary to the resolution of each class member's claim.

[87] The Plaintiffs brought the Court's attention to the Privacy Commissioner's investigation report that states that the personal information contained on the USB key could, in the wrong hands, lead to identity theft or fraud.

[88] Next, the Plaintiffs refer to the expert's report of Mr. Nicholas Scheurkogel, a cyber-security expert. Mr. Scheurkogel confirms that the type of information contained on the USB key can be assessed and designated at a Protected B level according to Government of Canada policies and guidelines. This information, by definition, applies to information that "if compromised, could cause serious injury to an individual, organization or government".

[89] Mr. Scheurkogel highlights that it is unclear what investigative procedures and techniques were taken after the USB key went missing. “Without these details it is not possible to comment on the thoroughness of the investigation and what happened to the USB key”.

[90] The Plaintiffs argued that the lack of certain investigatory measures means that there is a possibility the USB key was stolen. The government has not ruled out theft.

[91] The Plaintiffs also argued that the evidence on how the government designated the information contained on the USB key, on the risk to individuals, and on how the information was collected, is sufficient to establish some basis in fact that there is a claim for negligence.

[92] The Plaintiffs presented evidence from the class registration database, where approximately 7% of individuals reported they suffered from identity theft as a result of the breach. Counsel stated that they are not relying on this evidence for the truth of its contents, but rather for some basis in fact that there might be damages.

[93] The Defendant, on the other hand, argues there is no basis in fact to establish that any class member suffered compensable damages. Any claims for damages are entirely speculative. The Plaintiffs’ affidavits do not provide any details, particulars or meaningful information about the damages claimed to establish that they are common to the proposed class members. The Plaintiffs offer speculation about harm that might or could exist, but do not provide the minimal evidence required for certification.

[94] With respect to the damages claimed for psychological harms, the Defendant argues the Plaintiffs fail to show the minimum evidence required at the common issues stage. Damages for stress and anxiety must be "serious and prolonged and rise above the ordinary annoyances, anxieties and fears" (*Saadati v Moorhead*, 2017 SCC 28, at para 37).

[95] The law is very clear that the Plaintiffs do not need to prove damages to a civil standard at certification (*Sweet*, at para 17). The Plaintiffs are required to show some basis in fact, which requires the advancement of some evidence.

(b) *Increased risk of theft*

[96] In Mr. Scheurkogel's view, the analysis of the investigation reveals several shortcomings which undercut the government's conclusions that "there was no evidence that the USB key was stolen, accessed for fraudulent purposes, or taken outside the office":

> (a) He notes that "[t]he affidavits and information provided does not detail the investigative efforts to any useful degree. The affidavits state that one occurred but there is no specific indication of when the investigation began, when it ended, what detailed efforts were made, what was considered, who was interviewed, and what technical measures were undertaken to check for the drive." In his view, this undercuts the strength of any conclusions since it is impossible to assess the thoroughness of the investigation.
>
> (b) He notes that the conclusion that there was no evidence that the USB key was taken outside the office is directly undercut by the search of the employees home, and the taxi used to take the employee home, since "the USB key was evidently taken with some frequency to the lawyer's home, or why would it have been searched; and, the office was searched, and the USB was not located. Clearly, the USB key had to have been removed from the office or it would still be there. Clearly, the lawyer in question used and accessed the USB on occasion from their residence."

> (c) He notes that there is no timeline for when the USB key was last accessed by the lawyer despite the investigators having the ability to do so. By identifying the unique ID associated with use of the USB key, the investigators could have determined where the lawyer last used it (presumably the time would coincide with a time the lawyer was at home or at the office) as well as "whether the device had been inserted anywhere else in the organization." He notes "This would have been important information to frame when specifically, the USB was lost or stolen. It would also have been relevant to rule out or confirm where the sensitive information could have been accessed from." It would also allow the investigators to understand who had access to the USB at the time it disappeared.
>
> (d) Finally, he notes that there is no evidence "that dark web monitoring occur[ed] to look for the emergence of any of the lost or stolen USB Data within criminal forums. This is an obvious step as the sale of Canadian data to criminal groups could occur where it may be monitored, particularly as the USB Data is of obvious value to criminal groups."

[97] With respect to the ongoing risks to class members, Mr. Scheurkogel states that "[t]he fact that [the USB key] did not turn up after the search is a data point that needs to be considered – the potential that the device was stolen has not been discounted. The common practice in IT security in Government is to consider potentially breached information to be breached until it is proven NOT to have been." In other words, the fact that it did not turn up after such a thorough physical search suggests that it was taken rather than that it was "lost". Mr. Scheurkogel points out that there is nothing in the evidence provided by the Defendant (other than a bald conclusion) that would rule out the possibility that the USB was targeted. From his expert view, the Defendant's description of its own activities is insufficient to rule out theft, which means that "[t] here is insufficient information to judge if the risk of harm was eliminated." He notes that, without further evidence, he cannot offer a conclusion as to whether class members have

suffered harm. However, he agrees that the six years of credit flag protection was excellent and that the harm was limited, assuming the investigation was executed diligently.

[98] The Defendant retained the services of Mr. Fred Cate, a Professor of Law at Indiana University. Mr. Cate prepared an expert report on the risk of harm to the affected individuals. His opinions include the following:

> (a) The evidence in this case suggests there was no access to the data at all and that no identity theft has occurred;
>
> (b) Breaches consisting of lost or stolen hardware or media do not appear to contribute in any statistically significant way to identity theft;
>
> (c) The financial risk from identity theft is borne primarily by financial institutions and other businesses; rarely do individuals suffer economic loss;
>
> (d) Stolen personal data are usually exploited quickly, within 'days' or 'months,' rather than 'years', and;
>
> (e) The six years of fraud flag service is far beyond what was necessary to protect the individuals whose data is on the missing USB drive.

[99] With all due respect, I give more weight to Mr. Cate's evidence over that of Mr. Scheurkogel.

[100] Mr. Scheurkogel's position, if followed by the Court, would have the effect of putting the evidentiary burden on the Defendant's shoulders. It would reverse the burden to require the Defendant to provide some evidence that damages did not occur. It would require the Defendant to prove, at a standard close to beyond reasonable doubt, that the USB key has not been targeted. That is not the test before me. The burden was that of the Plaintiffs to bring some basis in fact

that they are facing an increased risk of identity theft; the Plaintiffs have failed to do so. Mr. Scheurkogel states that there is no evidence the dark web was monitored to look for the emergence of any of the USB key content. Yet he does not say whether he, as a cyber-security expert, has done such a search and if so, what the result of that search was.

[101] Mr. Scheurkogel's evidence is also highly speculative and based on generalities. He does not address any of the concrete issues raised by Mr. Cate besides agreeing that the six years of credit flag protection was excellent and that the harm was therefore limited.

[102] Finally, as to the Plaintiffs' argument that approximately 7% of individuals reported that they suffered from identity theft because of the breach, this must be put in context. It is 163 of the 5045 (3.2%) proposed class members who registered with class counsel as interested in the proposed class action. It is therefore 7% of 3.2% that reported having suffered from identity theft, well below the 3% of the population that are generally victims of identity theft.

(c) *Distress and anxiety*

[103] In *Saadati v Moorhead*, 2017 SCC 28, the Supreme Court of Canada found that serious and prolonged emotional upsets that rise above the ordinary annoyances of life are considered personal injuries and are compensable without the need to establish a psychiatric diagnosis.

[104] I find that the Plaintiffs do not show any evidence that their damages for stress and anxiety are serious and prolonged, such that they rise above ordinary annoyances. While the Plaintiffs plead damages for "suffering, distress, humiliation, anguish, reduced trust, feelings of

lost privacy, and ongoing increased levels of stress", there is no evidence or particulars presented by the Plaintiffs that establish that these damages are more than disturbance or that they rise above the annoyances of everyday life.

[105] The Plaintiffs have not produced the minimal evidence required at the common issues stage to support the existence of compensable damages on an individual basis, or on a class-wide basis. The proposed representative plaintiffs do not provide such evidence; rather they state that their information has not been misused to the best of their knowledge.

[106] I also find that the Plaintiffs fail to meet the evidentiary threshold set it *Jensen FCA*, regardless of whether the pleaded damages constitute pure economic loss. The law is very clear that the Plaintiffs do not need to prove damages to a balance of probabilities at certification (*Sweet*, at para 17). However, the Plaintiffs are required to show some basis in fact, which requires the advancement of evidence.

[107] The Plaintiffs have not provided any evidence that any members of the putative class sustained damages as a result of the Defendant's actions. I agree with the Defendant that the Plaintiffs have only provided evidence of a speculative risk, rather than any real substantial risk. They provided evidence that some proposed class members purport to have suffered identity theft and expert evidence that theft of the USB key cannot be ruled out completely. This is insufficient to establish the minimum evidence required to support the existence of a claim in negligence or to establish that the resolution of this common issue is necessary.

(d) *Aggregate damages*

[108] In *Pro-Sys*, the Supreme Court of Canada found aggregate damages questions to be appropriate for certification (at para 128).

[109] In the *Condon* and *Doe* files, this Court found aggregate damages questions to be appropriate for certification. This Court may order aggregate damages in the appropriate circumstances pursuant to Rule 333.28.

[110] The Defendant argues that the Plaintiffs must demonstrate with supporting evidence that there is a workable methodology for determining issues on a class-wide basis and without proof from individual class members. In *Canada v Greenwood*, 2021 FCA 186, the Federal Court of Appeal found there was no basis in fact for a common question on aggregate damages because the Plaintiffs failed to tender evidence to show how to conduct such an assessment (at para 188).

[111] I agree with the Defendant that the Plaintiffs have not discharged their burden of providing the Court with a basis in fact for a common question on aggregate damages. The Plaintiffs have not tendered evidence to show how the Court could conduct such an assessment.

D. *Is a class proceeding the preferable procedure for the just and efficient resolution of the common questions?*

[112] Paragraph 334.16(1)(d) of the Rules provides that a proposed class proceeding must be "the preferable procedure for the just and efficient resolution of the common questions of law or fact".

[113] The following non-exhaustive list must be considered when determining whether a class proceeding is preferable (Subrule 334.16(2)):

> a) The questions of law or fact common to the class members predominate over any questions affecting only individual members;
>
> b) A significant number of the members of the class have a valid interest in individually controlling the prosecution of separate proceedings;
>
> c) The class proceeding would involve claims that are or have been the subject of any other proceeding;
>
> d) Other means of resolving the claims are less practical or less efficient; and
>
> e) The administration of the class proceeding would create greater difficulties than those likely to be experienced if relief were sought by other means.

[114] With respect to factor (a), the Defendant does not contest that there are common questions pertaining to the law and fact of the Defendant's negligence in handling the Plaintiffs' personal information. The common questions pertaining to negligence predominate over individual claims.

[115] However, the other factors in Rule 334.16(2) do not militate in favour of a class.

[116] There is no evidence that a significant number of the members of the class have a valid interest in individually controlling the prosecution of separate proceedings.

[117] In addition, nearly 12 years have passed since the USB key was lost and there is no evidence of harm to the representative plaintiffs or indication of any improper use of the information. As indicated in Mr. Cate's expert opinion, the putative class is at no greater risk of identity theft because of the loss.

[118] The vast majority, if not all, of the individual claims being barred by the lapse of the statutory limitation period, a class proceeding cannot be used to revive these claims and it would not be in the interest of justice to certify a class action solely for the benefit of the three plaintiffs representatives.

[119] Finally, a class proceeding in this case would not serve the goal of behavioural modification; Employment Canada already took steps to change its policies and practices after having timely informed the affected individuals and the Privacy Commissioner that an employee had misplaced a USB key; they applied the Privacy Commissioner's recommendations, and; because of the passage of time since the incident and changes in technology, the goal of behaviour modification is not served by certification of this proposed class action.

VI. Conclusion

[120] Because the vast majority, if not all, of the class members' claims are statute barred due to lapsed limitation periods, but also because I find that the Plaintiffs do not meet the conjunctive test for certification, their motion is dismissed.

[121] The Defendant does not seek costs and none will be granted.

ORDER in T-226-13

THIS COURT ORDERS that:

1. The Plaintiffs' motion for certification is dismissed;

2. No costs are granted.

"Jocelyne Gagné"
Associate Chief Justice

FEDERAL COURT

SOLICITORS OF RECORD

DOCKET:	T-226-13
STYLE OF CAUSE:	JOHN MARK JACQUES, GORDON ALBERT MEHEW, and CRAIG ROBAR v HIS MAJESTY THE KING
PLACE OF HEARING:	TORONTO, ONTARIO
DATE OF HEARING:	MARCH 18-19, 2024
ORDER AND REASONS:	GAGNÉ A.C.J.
DATED:	JUNE 6, 2024

APPEARANCES:

Theodore P. Charney Caleb Edwards	FOR THE PLAINTIFFS
Sean Stynes Sarah Rajguru	FOR THE DEFENDANT

SOLICITORS OF RECORD:

Charney Lawyers PC Toronto, ON	FOR THE PLAINTIFFS
Strosberg Sasso Sutts LLP Windsor, ON	
Branch MacMaster LLP Vancouver, BC	
Bob Buckingham Law St. John's, NL	
Attorney General of Canada Ottawa, ON	FOR THE DEFENDANT