Federal Court  Cour fédérale

Date: 20220825

Docket: T-982-20

Citation: 2022 FC 1228

Ottawa, Ontario, August 25, 2022

PRESENT: The Honourable Mr. Justice Southcott

CERTIFIED CLASS ACTION

BETWEEN:

TODD SWEET

Plaintiff

and

HER MAJESTY THE QUEEN

Defendant

ORDER AND REASONS

I. Overview

[1] This decision relates to a motion by the Plaintiff dated December 2, 2021, seeking an order certifying this action as a class proceeding under Rule 334.16 of the *Federal Courts Rules*, SOR/98-106 [the Rules] and granting an order under Rule 334.17. This action relates to data

breaches in which hacker(s) gained access to the personal, financial and other information of what appears to be thousands of Canadians through Government of Canada websites.

[2] As explained in greater detail below, the Plaintiff's motion is granted, because I have found that the Plaintiff has satisfied the requirements of Rule 334.16.

II. **Procedural Background**

[3] The Plaintiff, Todd Sweet, is the proposed class representative for the proposed class proceeding. He is a resident of Clinton, British Columbia. The Defendant, Her Majesty the Queen, is named as representative of the Government of Canada [the Government] including the Minister of National Revenue of Canada (the Minister responsible for the Canada Revenue Agency [CRA]) and the Minister of Families, Children, and Social Development (the Minister responsible for Employment and Social Development Canada [ESDC]).

[4] The Plaintiff asserts that, on July 2, 2020, he logged in to his CRA online account after receiving emails notifying him that his email address had been removed from his account. He discovered that his direct deposit information had been changed and that, on June 29, 2020, using his account, an unknown and unauthorized individual had made four applications for the Canada Emergency Response Benefit [CERB], a program initiated by the Government to provide financial assistance to qualifying Canadians during the COVID-19 pandemic.

[5] The Plaintiff is one of a potential class of what appears to be thousands of people whose online Government accounts (including CRA accounts [styled for users as My Accounts], My

Service Canada Accounts for which ESDC is responsible, and other online accounts accessed via the Government of Canada Branded Credential Service Key [GCKey]) were vulnerable to hackers from approximately June to August of 2020, due to what the Plaintiff alleges were operational failures by the Defendant to properly secure the portals providing access to these accounts. The Plaintiff further alleges that, by obtaining unauthorized access to those accounts, hacker(s) were able to commit identity theft and CERB fraud and access sensitive and personal information including, e.g., Social Insurance Numbers [SINs], direct deposit banking information, tax information, dates of birth, records of employment, information regarding employment insurance, and other benefits information.

[6] On August 24, 2020, the law firm Murphy Battista LLP [Murphy Battista] commenced this action in the Federal Court on behalf of proposed class representatives who alleged that their online Government accounts had been accessed by hackers. However, in early April 2021, that firm experienced its own data breach, in which unauthorized parties were able to gain access to the firm's networks. The Defendant subsequently brought a motion to stay this action, because the Federal Court lacks the jurisdiction to hear a third party claim that the Defendant intended to pursue against the law firm, seeking contribution and indemnity in relation to any liability of the Defendant to members of the proposed class who may have had their information compromised in both the Government data breaches and the law firm data breach.

[7] Present Plaintiff's counsel, Rice Harbut Elliott LLP [Rice Harbut], subsequently replaced Murphy Battista and, in opposing the Defendant's stay motion, prepared pleading amendments intended to narrow the proposed class and the scope of its claim (to exclude persons who

contacted Murphy Battista about this class action) such that the Defendant would no longer have a basis to assert its claim for contribution and indemnity. Those amendments culminated with a draft Third Amended Statement of Claim [Third SOC], which would also replace the previously proposed class representatives with Mr. Sweet as Plaintiff.

[8] This proceeding is being case managed by the undersigned and Associate Justice Ring. By Order and Reasons dated December 20, 2021, I dismissed the Defendant's stay motion and, by Order dated January 20, 2022, I approved the filing of the Third SOC and the substitution of Mr. Sweet as the proposed representative Plaintiff for the class.

[9] The parties subsequently completed the service and filing of their records for the certification motion, which they argued orally in Vancouver on May 11-13, 2022. The Plaintiff's filings culminated with a Reply Memorandum of Fact and Law, which attached a draft Fourth Further Amended Statement of Claim [Fourth SOC] that the Plaintiff seeks leave to file (opposed by the Defendant) in the event the amendments therein are necessary to respond to certain of the Defendant's arguments. The Plaintiff seeks certification of a class defined as follows (with the underlined portion representing the only change from the Third SOC to the Fourth SOC):

> All persons whose personal or financial information in their Government of Canada Online Account was disclosed to a third party without authorization on or after March 1, 2020, excluding Excluded Persons.
>
> "Government of Canada Online Account" means:
>
> a) Canada Revenue Agency account;
>
> b) My Service Canada account; or

> c) another Government of Canada online account, where that account is accessed using the Government of Canada Branded Credential Service (GCKey).
>
> "Excluded Persons" means all persons who contacted Murphy Battista LLP about the CRA privacy breach class action, with Federal Court file number T-982-20 prior to June 24, 2021.
>
> (Collectively "Class" or "Class Members")

[10] The Plaintiff advances causes of action against the Defendant based on the torts of systemic negligence, breach of confidence, and intrusion upon seclusion, as well as invoking the vicarious liability provisions of the *Crown Liability and Proceedings Act*, RSC 1985, c C-50. He pleads that he and the other class members have suffered damages including: costs incurred in preventing identity theft; identity theft; increased risk of future identity theft; damage to credit reputation; mental distress and comparable effects; monies withdrawn from their bank accounts without their consent; loans applied for in their names without their consent; credit card fraud; inability to access benefits and payments they were entitled to and other losses resulting therefrom; out-of-pocket expenses; time lost in communication with the CRA, ESDC and other Crown agencies to address the data breaches; and time lost in precautionary communications with third parties such as credit agencies to inform them of the potential that personal and financial information may have been compromised.

[11] The present motion seeks an order certifying this action as a class action and granting an order under Rule 334.17 in connection with such certification. This includes certifying the following proposed common questions:

Systemic Negligence

A. Did the Defendant owe the Class a duty of care?

B. If so, what was the applicable standard of care?

C. Did the Defendant breach the applicable standard of care?

D. Did the Defendant's breach of duty cause damage to the Class?

Breach of Confidence

A. Is the Defendant liable for the tort of breach of confidence vis-à-vis Class Members?

Intrusion Upon Seclusion

A. Is the Defendant liable for the tort of intrusion upon seclusion vis-à-vis Class Members?

Damages

A. Can the Court make an aggregate assessment of all or part of the damages suffered by Class Members and, if so, in what amount?

B. Does the conduct of the Defendant merit an award of punitive damages and, if so, in what amount?

[12] The Defendant takes the position that the request for certification should be denied, arguing that none of the requirements for certification are met. The Defendant has also filed motions, asking that the Court strike an affidavit of one of the Plaintiff's factual witnesses (Elizabeth Emery) and strike certain paragraphs of the report of one of the Plaintiff's experts (Dr. Douglas Allen) or alternatively ascribe little weight to such evidence. These motions were argued at the commencement of the hearing of the certification motion and are addressed in these Reasons.

III. **Issues**

[13] Based on the parties' written and oral submissions, the issues for the Court's determination are as follows:

A. Should the Court strike certain paragraphs of Dr. Allen's expert report?

B. Should the Court strike the affidavit of Elizabeth Emery?

C. Has the Plaintiff satisfied the criteria of Rule 334.16, such that this proceeding should be certified?

[14] I note that the Plaintiff's Memorandum of Fact and Law raised as additional issues whether Rice Harbut should be appointed as class counsel and whether the Defendant should be required to disclose to Rice Harbut and the notice provider the names, mailing addresses, and email addresses of all class members, where that information is within the knowledge of the Defendant. However, the appointment of Rice Harbut has already been confirmed in my Order dated January 20, 2022, and at the hearing of the present motion, the Plaintiff's counsel advised

that he was advancing no particular submissions on the disclosure issue at this juncture. Counsel proposed that, if the proceeding is certified, this issue can be addressed subsequently through the case management process. This Judgment and Reasons therefore do not address that issue.

IV. **Analysis**

A. *General Principles*

[15] Before turning to analysis of the issues, it is useful to set out some general principles that apply to the certification of class proceedings. As I understand it, none of these principles are in dispute between the parties. This motion is governed principally by Rules 334.16(1) and (2), which provide as follows:

Certification	**Autorisation**
Conditions	**Conditions**
334.16 (1) Subject to subsection (3), a judge shall, by order, certify a proceeding as a class proceeding if	**334.16 (1)** Sous réserve du paragraphe (3), le juge autorise une instance comme recours collectif si les conditions suivantes sont réunies :
(a) the pleadings disclose a reasonable cause of action;	**a)** les actes de procédure révèlent une cause d'action valable;
(b) there is an identifiable class of two or more persons;	**b)** il existe un groupe identifiable formé d'au moins deux personnes;
(c) the claims of the class members raise common questions of law or fact, whether or not those common questions predominate over questions affecting only individual	**c)** les réclamations des membres du groupe soulèvent des points de droit ou de fait communs, que ceux-ci prédominent ou non sur ceux qui ne

members;

(d) a class proceeding is the preferable procedure for the just and efficient resolution of the common questions of law or fact; and

(e) there is a representative plaintiff or applicant who

(i) would fairly and adequately represent the interests of the class,

(ii) has prepared a plan for the proceeding that sets out a workable method of advancing the proceeding on behalf of the class and of notifying class members as to how the proceeding is progressing,

(iii) does not have, on the common questions of law or fact, an interest that is in conflict with the interests of other class members, and

(iv) provides a summary of any agreements respecting fees and disbursements between the representative plaintiff or applicant and the solicitor of

concernent qu'un membre;

d) le recours collectif est le meilleur moyen de régler, de façon juste et efficace, les points de droit ou de fait communs;

e) il existe un représentant demandeur qui:

(i) représenterait de façon équitable et adéquate les intérêts du groupe,

(ii) a élaboré un plan qui propose une méthode efficace pour poursuivre l'instance au nom du groupe et tenir les membres du groupe informés de son déroulement,

(iii) n'a pas de conflit d'intérêts avec d'autres membres du groupe en ce qui concerne les points de droit ou de fait communs,

(iv) communique un sommaire des conventions relatives aux honoraires et débours qui sont intervenues entre lui et l'avocat inscrit au dossier.

record.

Matters to be considered

(2) All relevant matters shall be considered in a determination of whether a class proceeding is the preferable procedure for the just and efficient resolution of the common questions of law or fact, including whether

(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.

Facteurs pris en compte

(2) Pour décider si le recours collectif est le meilleur moyen de régler les points de droit ou de fait communs de façon juste et efficace, tous les facteurs pertinents sont pris en compte, notamment les suivants :

a) la prédominance des points de droit ou de fait communs sur ceux qui ne concernent que certains membres;

b) la proportion de membres du groupe qui ont un intérêt légitime à poursuivre des instances séparées;

c) le fait que le recours collectif porte ou non sur des réclamations qui ont fait ou qui font l’objet d’autres instances;

d) l’aspect pratique ou l’efficacité moindres des autres moyens de régler les réclamations;

e) les difficultés accrues engendrées par la gestion du recours collectif par rapport à celles associées à la gestion d’autres mesures de redressement.

[16] As a general statement of the objectives of class action legislation, Chief Justice McLachlin provided the following explanation in *Hollick v Toronto (City)* 2001 SCC 68 at para 15:

> 15 The Act reflects an increasing recognition of the important advantages that the class action offers as a procedural tool. As I discussed at some length in *Western Canadian Shopping Centres* (at paras. 27-29), class actions provide three important advantages over a multiplicity of individual suits. First, by aggregating similar individual actions, class actions serve judicial economy by avoiding unnecessary duplication in fact-finding and legal analysis. Second, by distributing fixed litigation costs amongst a large number of class members, class actions improve access to justice by making economical the prosecution of claims that any one class member would find too costly to prosecute on his or her own. Third, class actions serve efficiency and justice by ensuring that actual and potential wrongdoers modify their behaviour to take full account of the harm they are causing, or might cause, to the public. …

[17] Other than the first requirement of Rule 334.16(1)—that the pleadings disclosing a reasonable cause of action, the test for which will be explained later in these Reasons—the threshold for meeting the requirements for certification is the establishment of "some basis in fact" to support the certification order. The law is clear that the "some basis in fact" threshold does not require that the party seeking certification establish the certification requirements on a balance of probabilities. Indeed, this standard does not require that the Court resolve conflicting facts and evidence at the certification stage. Rather, it 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 (see *Pro-Sys Consultants Ltd v Microsoft Corporation*, 2013 SCC 57 [*Pro-Sys*] at paras 101-102).

B. *Should the Court strike certain paragraphs of Dr. Allen's expert report?*

[18] The Plaintiff's certification motion record includes a report dated December 11, 2020, by Dr. Douglas Allen, an economist with Delta Economic Group Inc. As identified in his report, Dr. Allen was instructed to address two questions:

A. What would an economist consider is the scope of costs associated with identity theft?

B. What methodologies exist to estimate an average cost of this particular identity theft?

[19] The Plaintiff relies on Dr. Allen's evidence as relevant to the following proposed common issue that he seeks to certify:

> Can the Court make an aggregate assessment of all or part of the damages suffered by Class Members and, if so, in what amount?

[20] In response to Dr. Allen's report, the Defendant's motion record includes a report dated July 13, 2021, by Chris Polson and Jake Dwhytie of PricewaterhouseCoopers LLP [the PWC Report]. The Plaintiff in turn served a reply report by Dr. Allen dated July 22, 2021. The Defendant subsequently cross-examined Dr. Allen on both his reports.

[21] The Defendant's motion relates to the first of Dr. Allen's report [the Allen Report] and seeks:

A. to strike certain paragraphs on the basis that they violate a jurisprudential prohibition, applicable at the certification stage of a proceeding, against introducing evidence quantifying damages; and

B. to strike certain other paragraphs on the basis that they violate a jurisprudential prohibition, applicable at the certification stage of a proceeding, against using a random sampling of actual class members to calculate damages.

[22] Invoking the criteria prescribed by *R v Mohan*, [1994] 2 SCR 9, 114 DLR (4th) 419 [*Mohan*] for the admissibility of expert evidence, the Defendant argues that these two sets of paragraphs of the Allen Report are inadmissible, because they are both irrelevant and unnecessary to assist the Court in deciding the certification motion.

[23] First, the Defendant challenges paragraphs 12a, 14a, 21a (last sentence), 26-28, 31 and 38 of the Allen Report. These paragraphs relate to the first of two methodologies the Allen Report proposes for estimating the average cost of the identify theft that is the subject of this action. That methodology involves using information that is publicly available from a random sampling survey on identity theft. Dr. Allen explains how such information could be employed in that quantification methodology, including arriving at what he refers to as a base or floor estimate of the average cost per person.

[24] The Defendant recognizes that the Court can consider at the certification stage whether aggregate damages can be considered a common issue, but it emphasizes that the quantification

of damages is not a matter to be considered at this stage. The Defendant relies, *inter alia*, on *Pro-Sys* at paras 113-115, which noted that, during a certification proceeding, a court may contemplate whether loss to the class members can be established on a class-wide basis and that this process may require the use of expert evidence. However, the Supreme Court explained that it is not necessary at the certification stage that the methodology establish the actual loss to the class, only that that there is a methodology capable of doing so.

[25] Against this jurisprudential backdrop, I do not find the first set of impugned paragraphs of the Allen Report problematic. The Plaintiff offers that evidence not for the purpose of quantifying his damages or those of the proposed class members but rather to support his position that there is an available methodology for quantifying the class members' damages on an aggregate basis. This is a purpose expressly contemplated by *Pro-Sys* as relevant to the certification stage of a proceeding. As explained by the Court of Appeal for Ontario in *Fulawka v Bank of Nova Scotia*, 2012 ONCA 443 [*Fulawka*] at para 81 (cited by the Federal Court in *McCrea v Canada (Attorney General)*, 2015 FC 592 [*McCrea*] at para 351), a plaintiff is required to adduce supporting evidence to demonstrate that there is a workable methodology for determining issues of causation or damages, if proposed, on a class-wide basis.

[26] Next, the Defendant argues that paragraphs 14b, 32-36, and 39 of the Allen Report are inadmissible for violating a certification stage prohibition against using a random sampling of actual class members to calculate damages. As previously noted, Dr. Allen proposes two methodologies for calculating damages. The second methodology involves conducting a survey

of a random sample of class members. The Defendant submits that such a methodology is prohibited by law, because it requires proof by individual class members.

[27] In support of this position, the Defendant relies on the decision of the Court of Appeal for Ontario in *Fulawka* at paragraph 137, which rejected an expert's random sampling methodology because it impermissibly required proof from individual class members in order to arrive at an aggregate damages figure. The Court reasoned that this methodology was antithetical to the requirement in s 24(1)(c) of the *Ontario Class Proceedings Act, 1992*, SO 1992, c 6 [the Ontario Act], which authorizes a common issues trial judge to assess damages on an aggregate basis where the aggregate amount of the defendant's liability can reasonably be determined without proof by individual class members.

[28] In response, the Plaintiff identifies other authorities from courts in Ontario and British Columbia that he argues support his position that *Fulawka* is a jurisprudential outlier on the point on which the Defendant relies. These authorities include a recent decision of the Ontario Superior Court of Justice in *Fresco v Canadian Imperial Bank of Commerce*, 2020 ONSC 4288 at paras 20-22, in which Justice Belobaba described the decision on this point in *Fulawka* as an outlier, inconsistent with other jurisprudence of the Court of Appeal for Ontario and the language of the Ontario Act. Justice Belobaba invited the Court of Appeal to revisit this point.

[29] However, in the appeal from Justice Belobaba's decision, the Court of Appeal for Ontario declined this invitation, neither affirming nor departing from *Fulawka* (see *Fresco v Canadian Imperial Bank of Commerce*, 2022 ONCA 115 at paras 89-90). The Court concluded that any

ruling on the disputed point would have to wait until the completion of the plaintiff's proposed damages report, when it would be known whether statistical sampling would be used to fill any evidentiary gaps.

[30] While these cases upon which the Plaintiff relies may suggest that the law in Ontario on this point is somewhat unsettled, it remains the case that *Fulawka* represents the most recent pronouncement on the law in Ontario by its Court of Appeal. However, I find compelling the Plaintiff's argument that *Fulawka* is based on a provision of the Ontario Act that does not appear in the Rules of the Federal Court that apply to the present proceeding. The Defendant acknowledges that the Rules do not contain a provision similar to s 24(1)(c) but argues that, in *McCrea* at para 351, the Federal Court explicitly reviewed and adopted the principles of certification set out in *Fulawka*.

[31] In my view, *McCrea* does not assist the Defendant, who relies on Justice Kane's summary at paragraphs 350-352 of a list of principles set out at paragraph 81 of *Fulawka* regarding the establishment of a common issue. *McCrea* does not refer to, and I do not read it as necessarily endorsing, the analysis at paragraph 137 of *Fulawka*, based on s 24(1)(c) of the Ontario Act, upon which the Defendant's argument relies.

[32] The Plaintiff notes that Rule 348.28 addresses the Federal Court's authority to make aggregate assessments in class proceedings as follows:

334.28 (1) A judge may make any order in respect of the assessment of	**334.28 (1)** Le juge peut rendre toute ordonnance relativement à l'évaluation d'une

monetary relief, including aggregate assessments, that is due to the class or subclass.	réparation pécuniaire, y compris une évaluation globale, qui est due au groupe ou au sous-groupe**.**
…	…
(3) For the purposes of this rule, a judge may order any special modes of proof.	**(3)** Pour l'application de la présente règle, le juge peut ordonner le recours à des modes de preuve spéciaux.

[33] I agree with the Plaintiff's submission that these provisions do not include the restriction found in s 24(1)(c) of the Ontario Act. Indeed, Rule 334.28(3) expresses in broad terms the Court's authority to order special modes of proof in connection with an aggregate assessment.

[34] The Plaintiff also notes that, in *Cuzzetto v Business in Motion International Corporation*, 2014 FC 17 [*Cuzzetto*] at paras 102-103, Justice Rennie (then of the Federal Court) cited Rule 334.28 and stated that aggregate damages awards are available even if identifying class members who would be entitled to an award would be impractical or would require a case-by-case analysis. This statement appears inconsistent with the principle from *Fulawka* upon which the Defendant relies. Moreover, Justice Rennie explained in *Cuzzetto* that some guidance as to the appropriate amount of an aggregate award could be derived from an analysis which included data provided by class members in response to a survey conducted by counsel (at paras 99, 100, and 106).

[35] The Defendant also advances an argument that the prohibition against random sampling described in *Fulawka* should apply to this proposed class proceeding, because there is no

commonality among the proposed class members in relation to any damages to which they might be entitled as a result of the data breaches. Therefore, says the Defendant, a methodology employing a random sampling of the losses of actual class members would not assist the Court in accurately calculating aggregate damages.

[36] In my view, this argument does not speak to the admissibility of Dr. Allen's evidence. It is available to the Defendant to take the position on the main certification motion that the test for identification of common issues, including the application of that test to the proposed aggregate damages issue in particular, is not met. However, I do not see how this argument supports a conclusion that the impugned paragraphs of the Allen Report are inadmissible pursuant to a prohibition that is absent from the Rules.

[37] In relation to both sets of impugned paragraphs, I find that the evidence in the Allen Report is relevant to the Court's task of determining whether to certify the proposed common issue surrounding aggregate damages. I also accept the Plaintiff's submissions that economic models for assessing the cost of identity theft are beyond the ordinary understanding of a Court. I therefore consider the impugned evidence to satisfy both the relevance and necessity criteria of *Mohan*.

[38] The Defendant notes that Dr. Allen acknowledged in cross-examination that his report is based on certain assumptions, including that all losses suffered by the proposed class members resulted from the data breaches at issue, that the harm suffered was common throughout the class, that the Court has already found that the Defendant had a common duty to the class, and

that the Court has ruled in the Plaintiff's favour concerning causation and the applicable standard of care. The Defendant argues that such assumptions are prejudicial, because they depend on a finding of liability not yet made. The Defendant also submits that is it prejudicial for the Allen Report to be presenting a quantification figure.

[39] I find no merit to these arguments. It is not uncommon for an expert to make assumptions about the resolution of factual or legal issues upon which the expert is not personally opining. Obviously, if the assumptions turn out to be inaccurate, that may undermine the value of the opinion on the issue on which the expert is opining or indeed may eliminate that issue. However, I disagree with the Defendant's position that the fact the assumptions underlying the opinion are favourable to one party serves to prejudice the other party and thereby render the opinion inadmissible. The Court is capable of recognizing assumptions for what they are.

[40] Similarly, the fact that the Allen Report arrives at a floor or base quantification figure in demonstrating one of its proposed methodologies does not detract from the Court's ability to consider the methodological evidence, as distinct from its possible result, for the purpose that is relevant to the certification motion.

[41] I find the impugned paragraphs of the Allen Report admissible in the certification motion. The Defendant also relies on the evidence in the PWC Report in support of an argument that, if the impugned paragraphs are admitted, the Allen Report should be afforded little weight. I will return to that argument later in these Reasons, when analysing whether the Plaintiff has satisfied the criteria of Rule 334.16 such that this proceeding should be certified.

C. *Should the Court strike the affidavit of Elizabeth Emery?*

[42] The Defendant seeks to strike the second Affidavit of Elizabeth Emery, affirmed on July 23, 2021 [the Second Emery Affidavit], contained in the Plaintiff's reply motion record for certification on the basis that it fails to identify the source of the affiant's information and belief, is irrelevant to the certification criteria, contains unreliable opinion evidence, and constitutes improper reply.

[43] To place the Second Emery Affidavit in context, it is useful to explain briefly the evidentiary record before the Court in the certification motion. In its original motion record, the Plaintiff filed a number of affidavits from proposed class members (or those who would have been members of the proposed class before the change in the proposed definition explained above), a first affidavit from Ms. Emery (then an articled clerk and now a lawyer at Murphy Battista, the law firm representing the previous plaintiffs in this matter), and two expert reports (including the Allen Report referenced earlier in these Reasons). The Defendant's response includes affidavits from various government officials and expert reports of PricewaterhouseCoopers LLP (including the PWC Report referenced earlier in these Reasons). The Plaintiff's reply evidence contains additional affidavits including the Second Emery Affidavit.

[44] The Second Emery Affidavit appends various newspaper articles reporting on the wait times for the CRA helpline, the precautionary suspension of My Accounts by CRA in February and March of 2021, and the impact of CERB fraud on taxpayers' income tax. Ms. Emery also

appends a news release indicating that the Taxpayers' Ombudsperson will conduct a review of the communications CRA provided to taxpayers when it locked users out of their My Accounts in February 2021, as well as a statement from CRA regarding its decision to lock users' My Accounts to prevent unauthorized access.

[45] Ms. Emery states that her affidavit is affirmed in reply to the Defendant's responding motion record and specifically the PWC Report (which, as previously explained, responds to the Allen Report's opinion on methodologies for quantifying damages) and the affidavits of two government officials, Brian Rae and Mahmoud Gad.

[46] Mr. Rae is the Director, Digital Operations Division, in the Digital Services Directorate, Assessment, Benefit and Service Branch of CRA. His affidavit, affirmed June 8, 2021 [the Rae Affidavit] explains the CRA My Accounts; different ways to register for and log in to My Accounts; links between CRA and ESDC; My Accounts' security measures during the summer 2020 data breaches; CRA's disabling of online access and notification letters to affected individuals; CRA's timeframes for sending notification letters and follow-up letters; CRA's security check letters; its disabling of online access to My Accounts in February 2021; and the revocation of individual credentials in March 2021.

[47] Mr. Gad is a Senior Technical Advisor in the Information Technology Branch of CRA. In his affidavit affirmed June 30, 2021 [the Gad Affidavit], he addresses CRA's multi-layered security approach to the defence of its networks, systems, and portal applications against infiltration by hostile actors; login methods for CRA portal services; actions taken by CRA in response to the data breaches

(also described as cyber security incidents); details regarding the credential stuffing attack (explained later in these Reasons as the type of cyber security incidents involved in this matter); the impact of the cyber security incidents; the CRA information technology security analysis of whether individual affiant accounts were affected by the cyber security incidents; and the payment of CERB to individuals who qualified but did not receive it as a result of actions of bad actors. (I note that, in their evidence and submissions, the parties use the terms "hacker", "bad actor" and "threat actor" relatively interchangeably to refer to the person or persons who perpetrated the relevant data breaches.)

[48] In challenging the admissibility of the Second Emery Affidavit, the Defendant first argues that it consists entirely of hearsay evidence that is outside Ms. Emery's personal knowledge and is therefore inadmissible because it offends the requirements of Rule 81(1) by failing to identify the deponent's source of information and belief. Ms. Emery states in her affidavit that she has personal knowledge of the facts and matters deposed to therein. She also states that, where facts are not within her personal knowledge, she has stated the source of the information and believes that information to be true. However, the Defendant argues that these boilerplate statements do not satisfy Rule 81(1), which requires an explanation of the basis for a deponent's belief sufficient to demonstrate the reliability thereof (see, e.g., *Kish v Facebook Canada Ltd*, 2021 SKQB 198 at para 17; *Williams v Canon Canada Inc*, 2011 ONSC 6571 at para 102; *Thorpe v Honda Canada, Inc*, 2010 SKQB 39 at para 27).

[49] The Plaintiff's counsel admits that the boilerplate statements in the Second Emery Affidavit are inelegant but argue that this does not affect the admissibility of the evidence,

because it is not being relied upon for a hearsay purpose, i.e., to establish the truth of its contents. Therefore, Rule 81(1) does not apply. The Plaintiff relies on authority that, on a certification motion where the moving party need only establish that there is some basis in fact for the certification criteria, evidence can be admitted, even though it would not be admissible for the truth of its contents, in order to support, along with other evidence, that there is some basis in fact for those criteria (see, e.g., *Canada v Greenwood*, 2021 FCA 186 at para 96; *Johnson v Ontario*, 2016 ONSC 5314 [*Johnson*] at paras 54-67). As I summarized the conclusions in *Johnson* in *Tippett v Canada*, 2019 FC 869 [*Tippett*] at para 24:

> 24. The Plaintiff relies on the decision in *Johnson v Ontario*, 2016 ONSC 5314 at paras 54-67, which explained that, while a certification motion is not to be treated as an "evidentiary free for all," the procedural nature and purpose of the motion must be kept in mind. The Court held that, while the evidence contained in inquest material and newspaper articles, as well as an ombudsman report referenced therein, was not admissible for the truth of its contents, it could be considered and assessed, along with the frailties it may contain, to determine whether the moving party has met the onus of establishing some basis in fact for the certification requirements.

[50] Relying on these principles, I do not find the Second Emery Affidavit inadmissible based on the Defendant's hearsay arguments. For the same reasons, I reject the Defendant's arguments that the evidence is inadmissible because it includes unreliable opinions. To the extent the news articles attached as exhibits to the Second Emery Affidavit include statements of opinions, they are not at this stage of the proceeding being introduced for the truth of their contents, and their reliability is not presently at issue.

[51] The Defendant also submits that the Second Emery Affidavit should be struck because it is irrelevant to the issues in the certification motion and is not proper reply evidence. The Defendant asserts this argument first in relation to the evidence in the Second Emery Affidavit said to be offered in reply to paragraphs 66 to 71 of the Rae Affidavit, in which Mr. Rae explains that CRA disabled online accounts in February 2021 and revoked potentially compromised credentials in March 2021. The Defendant notes Mr. Rae's evidence that these measures related to accounts that were not compromised in the 2020 breaches. The Defendant therefore submits that the articles attached to the Second Emery Affidavit, reporting on taxpayers' reactions to these measures, are unrelated to the allegations in this proceeding. The Plaintiff responds that the Defendant cannot be certain that the risks to which CRA was responding in 2021 were unrelated to the 2020 breaches. I accept this submission, as the disputed articles include a Times Colonist report on the concerns of a taxpayer, reacting to being locked out of his account in February 2021, after having also been affected by CRA's data breach in August 2020.

[52] As to whether this evidence, related to taxpayers' reactions to the measures taken by CRA in February and March 2021, is proper reply, I am guided by the explanation in *Angelcare Development Inc v Munchkin, Inc*, 2020 FC 1185 at para 10 (quoting from *Halford v Seed Hawk Inc*, 2003 FCT 141):

> 10. From the principle against case splitting, Justice Pelletier in *Halford* draws a general rule on the scope of reply evidence, stating at paragraph 14 that:
>
> 14. <u>evidence which simply confirms or repeats evidence given in chief is not to be allowed as reply evidence</u>. It must add something new. But since the plaintiff is not allowed to split its case, that something new must be evidence which was not part of its case in chief. That can only leave evidence relating to matters

> arising in defence which were not raised in the plaintiff's case in chief. …
>
> [Emphasis in original.]

[53] The Defendant's materials responding to the certification motion describe the February and March 2021 measures as demonstrating proactive steps taken by CRA to contain and eradicate the cyber security incident. This evidence therefore relates to a matter arising in defence, and it is appropriate for the Plaintiff to reply with evidence on what he would characterize as adverse effects of those measures and potentially linking those measures to the 2020 data breaches. I therefore find that the paragraphs of the Second Emery Affidavit and related exhibits, offered in reply to paragraphs 66 to 71 of the Rae Affidavit, are admissible.

[54] However, I have reached the opposite conclusion on the evidence offered in reply to paragraphs 47 and 48 of the Rae Affidavit. In those paragraphs, Mr. Rae explains how CRA provided notification to some of the My Account holders affected by the 2020 data breaches, including security protocols to be employed when they contacted the CRA call centre in response to such notification. The Second Emery Affidavit references (at paragraph 2) and attaches (at Exhibits B and C) articles on lengthy wait times and resulting frustration experienced by callers. However, the Defendant points out that several of the proposed class member affiants provided evidence on their own similar experiences. The new evidence relates to a matter that was raised in the Plaintiff's evidence in its case in chief, and it is not appropriate to introduce more evidence on the same matter in reply. My Order will therefore strike paragraph 2 of the Second Emery Affidavit and the related Exhibits B and C.

[55] Finally, the Second Emery Affidavit seeks to introduce news articles about CERB fraud experienced by taxpayers who were affected by the data breach, including adverse tax consequences resulting from CERB payments being attributed to them as income. Ms. Emery says that this evidence is offered in reply to section 2.4 of the PWC Report and paragraphs 8 and 26 of the Gad Affidavit.

[56] I am satisfied that this new evidence is appropriate reply to paragraph 26 of the Gad Affidavit, which asserts that CRA has made whole and is continuing to make whole those who did not receive COVID-related benefits because payments had been made to bad actors through their accounts. While the Defendant points out that the proposed class member affiants provided evidence of concern about the effects upon them of CERB-related fraud, I read the new evidence as intended to cast doubt upon the Defendant's subsequent evidence to the effect that those affected were being made whole.

[57] To the extent the Defendant advances arguments in support of a position that, if the Second Emery Affidavit is admitted it should be afforded little weight, such arguments would be best addressed, if necessary, when analysing whether the Plaintiff has satisfied the criteria of Rule 334.16 such that this proceeding should be certified.

D. *Has the Plaintiff satisfied the criteria of Rule 334.16, such that this proceeding should be certified?*

(1) Factual Background

(a) *CRA's My Accounts*

[58] Before turning to the individual requirements for certification, it is helpful to canvass in more detail the factual background to the Plaintiff's action. As explained earlier in these Reasons, the effect of the "some basis in fact" threshold is that the Court is not required on a certification motion to weigh the evidence and make findings of fact. However, much of the factual background to this action appears to be undisputed. Indeed, both parties rely significantly on the evidence of the Defendant's affiants, including expert evidence, in explaining the nature of the online Government accounts, and the breaches thereof, underlying his action. The following summary is derived from the parties' explanations of the background in their respective Memoranda of Fact and Law. I will identify any factual components of this summary that I understand to be in dispute.

[59] As previously noted, CRA maintains an online portal, styled as My Account, that allows individual Canadian taxpayers to access CRA's services online and manage their tax affairs. Taxpayers can register for, and subsequently access, My Account, in three different ways: (a) through CRA's own Credential Management System [CMS]; (b) through a sign-in partner such as using a bankcard; or (c) through a BC Services Card. As will be explained in more detail below, only the first of these methods, using CRA's CMS, was affected by the data breaches that are the subject of this action. Registering for My Account using CRA's CMS involves an individual taxpayer creating a CRA user ID and password, as well as selecting five security questions and creating answers to those questions, following which CRA provides the taxpayer with a security code to be used to complete the registration process.

[60] When accessing My Account, the individual must enter the user ID and password and answer one of the security questions, which is randomly generated from among the five questions the individual selected during registration. The taxpayer can then view detailed tax information, including the status of tax returns, notices of assessment and reassessment, RRSP deduction limits, TFSA contribution room, and tax information slips, as well as personal information including addresses, telephone numbers, direct deposit banking information, marital status, and children in the taxpayer's care. The taxpayer can also apply for CERB and other benefits through My Account.

(b) *GCKey and ESDC's My Service Canada Accounts*

[61] Somewhat similarly, ESDC also maintains an online portal, styled as My Service Canada Accounts [MSCA], which individuals can use to access several ESDC programs, including Employment Insurance [EI], Canada Pension Plan [CPP] and Old Age Security [OAS] programs. Users can register for and subsequently access their MSCA through three methods: (a) using a GCKey credential; (b) using a sign-in partner; or (c) using a provincial digital identification in Alberta or British Columbia. Only the first of these methods, using GCKey, was affected by the data breaches that are the subject of this action.

[62] GCKey is a credential management service provided to the Government by a third party vendor named 2Keys Corporation [2Keys] and is intended to provide a single method of online access to many Government online services [Enabled Services]. GCKey assists over 30 Government departments, including ESDC; Parks Canada; Immigration, Refugees and

Citizenship Canada; Natural Resources Canada; and the Royal Canadian Mounted Police, in controlling access to over 100 Enabled Services. CRA does not use GCKey.

[63] To register for GCKey, a user chooses a username and password and requests a personal access code, which is used to complete the registration process. Subsequently, users can access GCKey through the username and password, described in the Defendant's Memorandum of Fact and Law as "single factor authentication". Unlike with CRA's My Accounts, there is no second step of answering a security question in order to access GCKey or to use GCKey to access MSCA. However, individual Government departments can implement additional security controls based on their specific Enabled Services.

[64] Once a user accesses MSCA through GCKey, the user can view tax information including tax slips, records of employment, information regarding EI applications, CPP, OAS, and other personal information including mailing addresses, telephone numbers, direct deposit banking information, names, SINs, and dates of birth. Significant to some of the data breaches underlying this action, at times material to the action a user accessing MSCA could also view and access all personal information contained in the user's CRA My Account, through an e-linking service between MSCA and My Account, without having to re-authenticate. In other words, a CRA My Account could be accessed using GCKey via MSCA, without having to answer the security question that would be required to access My Account directly.

[65] Like CRA's My Account, ESDC's MSCA represented a means by which users could apply for the CERB.

(c) *The Data Breaches*

[66] In the summer of 2020, GCKey and CRA's My Account were the subject of what the cybersecurity industry describes as a "credential stuffing attack" by a threat actor, predominantly targeting CRA and ESDC as a means of fraudulently applying for COVID relief benefits (CERB and the Canada Emergency Student Benefit [CESB]) that had been introduced by the Government in the spring of 2020). Credential stuffing is a form of cyber attack that relies on the use of stolen credentials (username and password) from one system to attack another system and gain unauthorized access to an account. This type of attack relies on the reuse of the same username and password combinations by people over several services. Threat actors sell lists of credentials on the Dark Web. Credential stuffing usually refers to the attempt to gain access to many accounts through a web portal using an automated bot system rather than manually entering the credentials. On dates in July 2020, CRA's My Account experienced large numbers of failed logins, which have since been identified as a precursor to, or otherwise part of, a credential stuffing attack against that service.

[67] A threat actor attempting to access a particular My Account through credential stuffing would typically have encountered the requirement to successfully answer one of the five security questions selected by the user. However, during the attack that occurred in the summer of 2020, the threat actor(s) were able to bypass the security questions, and access My Account, because of a misconfiguration in CRA's credential management software. CRA learned of this method to bypass the security questions on August 6, 2020, when it received a tip from a law enforcement partner that such a method was being sold on the Dark Web. Among other steps taken to respond

to the data breach, CRA subsequently identified the relevant misconfiguration in its software, which it remedied on or about August 10, 2020.

[68] In the meantime, at least 48,110 My Accounts were impacted by the unauthorized use of credentials, meaning that the threat actor was able to enter a valid CRA user ID and password. Of those 48,110 My Accounts, 21,860 involved no progress by the threat actor beyond entering the ID and password, such that the threat actor did not access the accounts. This is potentially understood as a stage of the attack in which the threat actor was ensuring that the credentials worked. The threat actor(s) actually logged in to 26,250 My Accounts. In 13,550 of the My Accounts, although the security question bypass was used, the threat actor only viewed the homepage, meaning that some personal information was accessed, but no application was submitted for CERB. In 12,700 of the My Accounts, the threat actor changed the relevant taxpayer's direct deposit banking information and fraudulently applied for CERB.

[69] The Defendant's expert evidence explains that post-incident analysis revealed that the credential stuffing attack against CRA's CMS system occurred between July 27 and August 10, 2020. I understand that, at least at this stage of the proceeding, the Plaintiff does not necessarily accept these temporal limits on the duration of the attack.

[70] CRA initially treated as potentially compromised any My Account where a valid set of credentials was used, even if the account was not actually accessed, and sent notification letters to the account holders, including offering enhanced protection services for a period at no cost.

[71] Turning to the attack on GCKey, the evidence is that on June 18, 2020, and on various dates in July 2020, it experienced large numbers of failed logins, which have since been identified as a precursor to, or otherwise part of, a credential stuffing attack against the GCKey service. 2Keys advised the Government on August 4, 2020 that they had noticed some login anomalies in the previous days, and August 5, 2020, 2Keys determined that the suspicious login activity was a large-scale credential stuffing attack on the GCKey service.

[72] ESDC is the Government department that suffered the greatest impact from the attack on GCKey. ESDC has identified 5,957 accounts across several Enabled Services that were potentially impacted by the attack, of which 3,439 accounts were accessed by someone (including potentially the rightful owner) between July 15 and August 5, 2020, including access for purposes of changing banking information or addresses. Subsequent analysis concluded that the remaining 2,518 of the 5,957 accounts showed no access. 3,200 compromised MSCAs were used to access CRA My Accounts via the link between MSCA and CRA, and 1,200 of those accounts were used to apply for CERB or other COVID-related benefits.

[73] Among other steps taken to respond to the data breach, the Defendant’s evidence is that, as of August 14, 2020, 2Keys was able to block all botnet traffic on the GCKey service and block the credential stuffing attack from occurring further. On August 14, 2020, ESDC also disabled the link between the MSCA and CRA My Account. Again, I understand that the Plaintiff does not necessarily accept this temporal limit on the duration of the attack.

[74] Between August 1, 2020, and August 25, 2020, ESDC sent notification letters to all affected ESDC account holders that use the GCKey service, informing them that their accounts may have been accessed as a result of the credential stuffing attack. ESDC offered two years of credit monitoring with Equifax to anyone whose information may have been accessed as a result of the attack.

(2) Disclosure of a Reasonable Cause of Action

[75] The first requirement for certification is that prescribed by Rule 334.16(1)(a), that the pleadings disclose a reasonable cause of action. 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 pleading discloses no reasonable cause of action. This analysis is not to be conducted based on evidence submitted by the parties, but rather based on the assumption that the facts as pleaded are true (see, e.g., *Condon v Canada*, 2015 FCA 159 [*Condon FCA*] at paras 11-13).

[76] The Plaintiff advances causes of action in systemic negligence, breach of confidence, and intrusion upon seclusion. The Defendant argues that the Plaintiff's pleadings do not disclose a reasonable cause of action in any of these torts. I will consider each proposed cause of action individually.

(a) *Systemic Negligence*

(i) The Parties' Positions

[77] Both the Third SOC and the Fourth SOC are materially identical in their framing of the Plaintiff's allegations of systemic negligence. They allege that the Defendant owed a common law and non-delegable duty to the Plaintiff and other Class Members to use reasonable care in the collection, storage, and retention of their personal and financial information and a duty to ensure that this personal and financial information was safe, kept private, and protected and that it would not be subject to unauthorized disclosure to a third party.

[78] The Plaintiff pleads s 8(1) of the *Privacy Act*, RSC 1985, c P-21, pursuant to which personal information under the control of the Defendant cannot, without the consent of the individual to whom the information relates, be disclosed by the Defendant, and asserts that the Defendant's breach of the *Privacy Act* is evidence that its conduct fell below the applicable standard of care.

[79] The pleadings articulate a number of alleged systemic breaches of the Defendant's duty by, among other things, failing to create or adhere to Government policies relevant to the collection, storage, retention and disclosure of personal and financial information; failing to take reasonable steps to protect such information; failing to offer a non-vulnerable security question mechanism for users of the GCKey, My Account, and MSCA systems; failing to follow industry norms regarding two factor authentication for these accounts; and failing to take reasonable steps, including freezing the online systems, when they knew or ought to have known of the data breaches.

[80] The pleadings assert that measures taken by the Defendant in the latter part of 2020 to protect its databases, systems and other relevant online accounts should have been taken prior to the unauthorized data breaches. They further assert that the Defendant's breaches caused the Plaintiff and other Class Members harm and ongoing damages, including distress, anxiety, mental anguish, lost time, lost opportunities, and out-of-pocket expenses.

[81] The Defendant raises a number of arguments in support of its position that the Plaintiff's pleadings do not disclose a reasonable cause of action in systemic negligence. The Defendant submits that the Plaintiff has failed to plead any facts to support a relationship of proximity necessary to establish a *prima facie* duty of care; that the negligence claim cannot succeed because it challenges a core policy decision that is immune from liability; and that the claim should fail because it seeks to impose a duty of care in circumstances that would result in indeterminate liability to an indeterminate class.

[82] The parties agree that the principles governing whether a duty of care will be recognized in a given case alleging liability of a public authority are those derived from *Anns v Merton London Borough Council*, [1978] AC 728 (HL) [*Anns*], as applied in *Cooper v Hobart*, 2001 SCC 79 [*Cooper*], and its companion case, *Edwards v Law Society of Upper Canada*, 2001 SCC 80 [*Edwards*]. As summarized in *Edwards* at paras 8-10:

> 8. The companion case of *Cooper* outlines the approach in assessing whether a duty of care will be recognized in a given case. Specifically, *Cooper* revisits the *Anns* test and clarifies the express policy components to be considered at each stage.
>
> 9. At the first stage of the *Anns* test, the question is whether the circumstances disclose reasonably foreseeable harm and proximity sufficient to establish a *prima facie* duty of care. The focus at this

> stage is on factors arising from the relationship between the plaintiff and the defendant, including broad considerations of policy. The starting point for this analysis is to determine whether there are analogous categories of cases in which proximity has previously been recognized. If no such cases exist, the question then becomes whether a new duty of care should be recognized in the circumstances. Mere foreseeability is not enough to establish a *prima facie* duty of care. The plaintiff must also show proximity — that the defendant was in a close and direct relationship to him or her such that it is just to impose a duty of care in the circumstances. Factors giving rise to proximity must be grounded in the governing statute when there is one, as in the present case.
>
> 10. If the plaintiff is successful at the first stage of *Anns* such that a *prima facie* duty of care has been established (despite the fact that the proposed duty does not fall within an already recognized category of recovery), the second stage of the *Anns* test must be addressed. That question is whether there exist residual policy considerations which justify denying liability. Residual policy considerations include, among other things, the effect of recognizing that duty of care on other legal obligations, its impact on the legal system and, in a less precise but important consideration, the effect of imposing liability on society in general.

(ii) Foreseeability

[83] Beginning with the first stage of the *Anns/Cooper* test, which considers both foreseeability and proximity, the Defendant relies on *Del Giudice v Thompson*, 2021 ONSC 5379 [*Del Giudice*], in support of its position that the harm to the Plaintiff and the proposed Class Members in the case at hand was not reasonably foreseeable. *Del Giudice* addressed a certification motion arising from the defendant Thompson's hacking of the database of personal information collected by the defendant banks and financial institutions and held on the servers of the defendant Amazon Web. As a consequence of this data breach, personal and confidential information of 106 million applicants for Capital One credit cards was exposed or became vulnerable to exposure to the public. Among their claims, the plaintiffs sought to certify causes

of action against Amazon Web in negligence and breach of a duty to warn of the risk of the data breach perpetrated by Thompson.

[84] In addressing the foreseeability of the harm suffered by the proposed class members, the Court relied on *Rankin (Rankin's Ranch & Sales) v JJ*, 2018 SCC 19 [*Rankin*], in which the Supreme Court considered the foreseeability of personal injury resulting from an unlicensed and inebriated minor operating a motor vehicle after stealing it from the defendant's garage. The Supreme Court accepted that the evidence could establish, as the jury found, that the defendant ought to have known of the risk of theft. However, the Court concluded that it did not automatically flow from evidence of the risk of theft in general that the garage owner should have considered the risk of physical injury. Rather, physical injury was foreseeable only if there was something in the facts to suggest not only a risk of theft, but that the stolen vehicle might be operated in a dangerous manner (at para 34).

[85] *Del Giudice* drew a parallel between the personal injury claim in *Rankin* and the claim against Amazon Web, concluding that, while Amazon Web could have foreseen the possibility of data it was storing being stolen and misused, that did not make the resulting harm a reasonably foreseeable consequence of its alleged carelessness (at para 241). In arriving at that conclusion, the Court reasoned that the wrong suffered by the class members was the data breach perpetrated by Thompson, which was not connected to a wrong perpetrated by Amazon Web.

[86] In my view, the reasoning in *Del Giudice* is not particularly compelling. I appreciate that, in both *Rankin* and *Del Giudice*, there was another party (respectively, the car thief and

Thompson) who was the immediate cause of the harm. However, I have difficulty with the parallel that *Del Giudice* draws with *Rankin*. As the Supreme Court reasoned in *Rankin*, the theft of property does not automatically translate into anticipation that the stolen property will be operated in a dangerous manner so as to cause personal injury (at para 34). However, *Del Giudice* does not explain why, in the case of a data breach, the risk of unauthorized use of data by the bad actor who wrongfully accessed it, presumably for personal gain, and the attendant harm to its owner should be regarded as similarly unanticipated.

[87] I agree with the Plaintiff's submission that, considering the authorities that analyse foreseeability in the context of a data breach, the reasoning of the Supreme Court of British Columbia in *Tucci v Peoples Trust Company*, 2017 BCSC 1525, [*Tucci*] (upheld on this point in *Tucci v Peoples Trust Company*, 2020 BCCA 246 [*Tucci BCCA*]) is the more persuasive. *Tucci* addressed a certification motion in an action alleging that the defendant trust company did not adequately secure personal information collected on its online application portal and stored in online databases. The plaintiff asserted causes of action, including negligence, alleging that unauthorized persons were able to access the personal information, putting the proposed class members at risk of identity theft and other harms. In applying the first stage of the *Anns/Cooper* test, including the foreseeability element, the Supreme Court of British Columbia held as follows (at para 123):

> 123 In my view it is not plain and obvious that the first stage of the *Anns/Cooper* test is not met. The plaintiff has pleaded sufficient facts capable of establishing that harm was reasonably foreseeable. The information collected by Peoples Trust was sensitive and collected in the course of online applications for financial services. It is arguably reasonably foreseeable that harm such as identity theft could result if such information were disclosed or not securely stored, and it was again arguably

> foreseeable to Peoples Trust given the various policies and contractual terms it developed. Further, the plaintiff has pleaded sufficient facts that could establish a close and direct relationship between Peoples Trust and individuals who applied to it for financial services.

[88] *Tucci BCCA* upheld this component of the analysis, concluding that the allegations of negligence were arguably sufficient at law to create a relationship giving rise to a duty of care, such that it was not plain and obvious at the certification stage of the proceeding that a negligence claim cannot succeed (at para 51).

[89] In the case at hand, the Plaintiff has pleaded that the online Government accounts of the proposed Class Members, which were the subject of the data breaches, contain detailed personal and financial information, including financial records, notices of assessment, banking information, information on income, disabilities, children, relationship status and investments, and information related to EI, immigration status, CPP and OAS. The Plaintiff also pleads that that the Defendant has policies and guidance on cybersecurity, which serve to impose responsibilities upon the Defendant and to which it failed to adhere. As in *Tucci*, I find that it is arguably reasonably foreseeable that that the proposed Class Members would suffer the categories of harm alleged by the Plaintiff as a result of the data breaches.

(iii) Proximity

[90] Still in connection with the first stage of the *Anns/Cooper* test, the Defendant also submits that the Plaintiff has not shown that proximity exists between the proposed Class Members and the Defendant such as would make it just to impose a duty of care in the

circumstances of this case. As noted above, *Edwards* explains at paragraph 9 that the starting point for this analysis is to determine whether there are analogous categories of cases in which proximity has previously been recognized. The Plaintiff argues that *Tucci* is such a case, as are *John Doe v Canada*, 2015 FC 916 [*John Doe*], *Condon FCA*, and *Obodo v Trans Union of Canada, Inc*, 2021 ONSC 7297 [*Obodo*]. The Defendant responds that these are all decisions on certification motions and therefore do not represent authority for the recognition of the requisite proximity and the resulting duty of care.

[91] *John Doe* addressed a certification motion in which the plaintiffs pleaded that the defendant Government identified them as participants in the Marijuana Medical Access Program by sending letters to them through the mail that identified that Program as the return address. In concluding that the proceeding should be certified, Justice Phelan held that the plaintiffs had adequately pleaded the requisite elements of negligence, including the duty of care, and that these pleadings were sufficient for purposes of the motion (at paras 33-36). *John Doe* was upheld on this point in *Canada v John Doe*, 2016 FCA 191 [*John Doe FCA*].

[92] Logically, I agree with the Plaintiff that, in order for the cause of action in negligence to have been certified in *John Doe*, the Court must have concluded that the requisite proximity existed. However, the decision contains no express analysis of this point, as it appears that the defendant was not arguing a lack of proximity. Moreover, *John Doe* is not a cybersecurity case, and its facts, in which it was the Government itself that was alleged to have disclosed personal information, without any involvement by a third-party bad actor, are sufficiently different from

those in the case at hand that I have difficulty treating it as an analogous case in which proximity has previously been recognized.

[93] In *Condon FCA*¸ the Federal Court of Appeal allowed an appeal from *Condon v Canada*, 2014 FC 250 [*Condon*], which had concluded that it was plain and obvious that a claim in negligence would fail. *Condon* involved a motion to certify a class proceeding against the Government resulting from its loss of an external hard drive on which it stored the personal information of participants in the Canada Student Loans Program. While the Federal Court certified the proceeding based on other causes of action, it accepted the defendant's position that the plaintiffs had failed to raise sufficient arguments as to the existence of compensable damages and therefore concluded that it was plain and obvious that a proposed claim based on negligence would fail (at paras 68 and 79).

[94] In *Condon FCA*, the Federal Court of Appeal held at paragraphs 15 to 18 that the Federal Court had erred by evaluating the evidence in concluding that the plaintiffs had not suffered any compensable damages and by failing to consider the pleaded claims for costs incurred in preventing identity theft and out-of-pocket expenses. As with *John Doe*, there is no express proximity analysis, as the defendant does not appear to have raised proximity as an impediment to certification, and the facts are sufficiently different from the present case that I would not regard *Condon FCA* as an analogous case in which proximity has previously been recognized.

[95] Unlike *John Doe* and *Condon*, *Obodo* is a cybersecurity case, arising from a large-scale intrusion by unknown and unauthorized persons into the database of the defendant Trans Union.

The hackers accessed the credit profiles of 37,444 individuals whose financial information was held by Trans Union. However, while challenging certification of the plaintiff's negligence claim on other bases related to the categories of damages claimed, Trans Union acknowledged that the claim disclosed facts sufficient to establish a breach of a duty of care (at paras 116-118). As such, *Obodo* does not provide any analysis of proximity.

[96] However, as reflected in paragraph 123 of *Tucci*, the Plaintiff is correct that in that case the Supreme Court of British Columbia found the required proximity, in that sufficient facts had been pleaded to establish a close and direct relationship between Peoples Trust and individuals who applied to it for financial services. As previously noted, the Court of Appeal for British Columbia agreed with this conclusion. As I read *Tucci,* the Court based its conclusion on pleaded facts to the effect that individuals applied to Peoples Trust for financial services and, in doing so, provided it with their sensitive financial information.

[97] In the case at hand, the Plaintiff similarly bases his proximity arguments on the fact that he and the proposed Class Members had applied or registered for the Government's secure portals. The Plaintiff submits that the requisite proximity is found in the relationship between Government entities who have offered online access to data and individuals who have availed themselves of that access and created profiles in the expectation that their personal and financial information would be kept secure.

[98] The Defendant acknowledges that one of the situations in which sufficient proximity may exist, for a government to owe a private law duty of care to an individual plaintiff, is where there

have been specific interactions between the government and the individual (see *R v Imperial Tobacco Canada Limited*, 2011 SCC 42 [*Imperial Tobacco*] at para 45). However, the Defendant argues that the Plaintiff has not pleaded facts that would support a finding of proximity on this basis.

[99] In response to this argument, the Plaintiff submits that the Third SOC identifies that he had a CRA online account that was breached and expressly defines the proposed Class as persons whose personal or financial information in their online Government accounts was disclosed to a third party. The Plaintiff has also provided in draft a Fourth SOC, which he seeks leave to file in the event the amendments therein are necessary to respond to the Defendant's argument. These amendments include a more express statement that the Plaintiff had an online account with CRA and that he signed up for and used the CRA My Account, to the mutual benefit of himself and the Defendant, the latter gaining benefit by automating functions that otherwise would require increased staffing and expense.

[100] In my view, the pleaded facts in the Third SOC, as identified in the Plaintiff's submission, sufficiently assert a basis for proximity consistent with that recognized in *Tucci*. I am conscious of the Defendant's argument that, as *Tucci* is a certification decision, it does not represent authority for past recognition of the requisite proximity in an analogous case as contemplated by the *Anns/Cooper* test. The Defendant also submits that the certification of negligence as a common issue does not preclude a defendant from arguing at a common issues trial that it does not owe a duty of care, including that no proximity exists with class members or that a duty could be negated by policy considerations.

[101] I agree with the Defendant's submission that these defence arguments would remain available to it at trial, notwithstanding success by the Plaintiff in certifying his action. Indeed, the Plaintiff does not disagree with the Defendant's position on this point, which naturally follows from the fact that the Court's conclusion on certification is only that it is not plain and obvious that the pleading discloses no reasonable cause of action. *Tucci* found that it was not plain and obvious that the first stage of the *Anns/Cooper* test was not met, and I consider that finding sufficient authority for a comparable finding in the case at hand.

[102] In so concluding, I am also conscious of the fact that *Tucci* involved a claim against a private sector defendant, and I acknowledge the Defendant's argument that, because of the breadth of public bodies' involvement in the collection of personal and financial information, imposing a duty of care to protect against unintended disclosures through cyber security incidents raises policy concerns of indeterminate liability. However, I consider that argument to be best addressed in the second stage of the *Anns/Cooper* test, and will do so later in these Reasons.

[103] Even if I were to conclude that *Tucci* is not sufficient authority for satisfaction of the first stage of the test, making it necessary for the Court to consider, without the benefit of previous authority, whether the Defendant was in a close and direct relationship to the Plaintiff and the proposed Class Members such that it is just to impose a novel duty of care in the circumstances, I would still find the first stage of the *Anns/Cooper* test to be met on the facts pleaded in this action. The Third SOC identifies the Plaintiff and the proposed Class as persons with online Government accounts containing personal and financial information. As previously noted, the

Plaintiff argues that the requisite proximity arises from the relationship between Government entities who have offered online access to data and individuals who have availed themselves of that access and created profiles in the expectation that their personal and financial information would be kept secure. In my view, this is a reasonably arguable position, such that it is not plain and obvious to me that the first stage of the *Anns/Cooper* test is not met.

[104] Before finishing with the first stage of the test, I will briefly address the Plaintiff's request for leave to file the Fourth SOC, which accompanied his Reply Memorandum of Fact and Law. I understand that request to be an alternative position, if necessary to respond to the Defendant's argument that the Third SOC does not plead facts sufficient to establish the requisite proximity. As I have found the Third SOC sufficient, I need not consider whether leave should be granted to make the amendments proposed in the Fourth SOC.

[105] Moreover, I am conscious of the Defendant's argument in resisting the Plaintiff's request for leave. By Order dated November 2, 2021 [Case Management Order], Associate Justice Ring ordered that a case management teleconference be requisitioned if the Plaintiff intended to make any further amendments to the Statement of Claim prior to the hearing of the certification motion. This was to ensure the proposed amendments and their impact on the litigation schedule could be discussed with the Court. The Defendant correctly asserts that the Plaintiff did not comply with the requirement in the Case Management Order. With the exception of an amendment to the proposed Class definition, which I will address later in these Reasons, I therefore decline to grant the Plaintiff leave to file its amendment. If, following the issuance of

this certification decision, the Plaintiff considers that a pleading amendment remains necessary, he can seek leave through the case management process.

(iv) Policy Considerations

[106] I therefore turn to the second stage of the *Anns/Cooper* test. In taking the position that there are applicable policy considerations that should serve to negate a duty of care, the Defendant first relies on the principle that a duty of care should not be found in connection with a core policy decision. As explained in *Nelson (City) v Marchi*, 2021 SCC 41 at paragraph 44, courts should not interfere with policy decisions, as this would represent second-guessing the decisions of democratically elected government officials. In *Imperial Tobacco* at paragraph 90, the Supreme Court concluded that core policy government decisions are decisions as to a course or principle of action that are based on public policy considerations, such as economic, social and political factors. These are protected from suit provided they are neither irrational nor taken in bad faith.

[107] The Defendant submits that it is clear from the Plaintiff's pleadings that his allegations essentially amount to a criticism of the Government's core policy decision to use existing systems to roll out the CERB and other COVID relief benefits at the beginning of the pandemic. In support of this argument, the Defendant refers to the Plaintiff's pleading as including the following:

A. that the timing of the first data breach correlated with the Government's introduction of the CERB program and the breaches continued through the period that COVID benefits were being offered;

B. that the online application system for CERB and CESB was implemented hastily and recklessly without taking necessary precautions to protect the Plaintiff's and Class Members' personal and financial information in their online Government accounts;

C. that the Defendant ought to have known that its databases and online systems were vulnerable to unauthorized breaches and failed to take timely and reasonable protective measures both before and after launching the online CERB and CESB programs; and

D. that CRA was aware of an increase in fraudulent activity at the beginning of each monthly CERB and CESB period and generally during the time at issue but did nothing to notify or warn the Plaintiff.

[108] The Defendant submits that the Government's decision to use existing systems to deliver COVID relief benefits achieved its intention of Canadians having broad accessibility to apply for and receive the benefits rapidly. The Defendant argues that this decision is therefore one of core policy, which is immune from liability.

[109] In response, the Plaintiff submits that, far from criticizing this decision, he considers it an admirable goal on the part of the Government to quickly deliver benefits to those in need. The Plaintiff argues that his allegations focus not on this decision but on what he asserts were inadequate security protocols in place for those Canadians who had elected to register for online services with CRA and other government accounts, expecting that their personal or financial information would be secure.

[110] I do not find the Defendant's argument particularly compelling. While the decision to employ existing systems to deliver COVID relief benefits could potentially be characterized as a policy decision, I have difficulty with the Defendant's position that the Plaintiff's allegations focus upon this decision. I accept that the Third SOC alleges a relationship between the introduction of the COVID benefits in the spring of 2020 and the subsequent cyber security incidents, both in terms of timing and the objectives of the threat actors. However, I find reasonably arguable the Plaintiff's position that his assertions of actionable errors or omissions on the part of the Defendant focus upon allegedly inadequate online security measures. As it will remain available to the Defendant to raise its policy argument at a common issues trial, I will not analyse this issue further other than that to conclude that it is not plain and obvious to me that this argument will negate the existence of a duty of care.

[111] I also note that, in *Ari v Insurance Corporation of British Columbia*, 2015 BCCA 468 [*Ari*], the Court of Appeal for British Columbia found that a duty of care should not be recognized for several public policy reasons. In *Ari*, at the core of the negligence claim as pleaded was the adequacy of security measures that the defendant undertook as a matter of policy pursuant to its statutory obligations to protect personal information in its custody (at para 52). The Court noted that the policy decisions of public bodies are not actionable in negligence. This case is distinguishable in that the Plaintiff's pleadings include allegations that the Defendant breached his duty by failing to adhere to its policies to ensure protection of his and the other Class Members' personal financial information. *Tucci* distinguished *Ari* on a similar basis (at para 131).

[112] Next, the Defendant submits that there are policy reasons negating a duty of care in that such a duty would raise the spectre of indeterminate liability on the part of the Government. As explained in *Alberta v Elder Advocates of Alberta,* 2011 SCC 24 at paragraph 74, the possibility of unlimited government liability to an unlimited class may tax public resources and chill governmental intervention. *Cooper* (at para 54) and *Imperial Tobacco* (at para 99) raise this concern in circumstances where a government has no control over the number of potential claimants.

[113] The Defendant relies on *Ari*, which addressed a motion to strike a claim arising from a breach of privacy by an Insurance Corporation of British Columbia [ICBC] employee. The claim alleged that ICBC breached its alleged duty by failing to have an adequate system in place to prevent unauthorized access to personal information. As previous noted, the Court of Appeal for British Columbia concluded that no duty of care could be recognized because of several policy concerns. These concerns included that recognizing a duty of care would raise the spectre of indeterminate liability (at para 50).

[114] In my view, the indeterminate liability argument is among the strongest of the Defendant's submissions in opposing the Plaintiff's certification motion. In *Tucci,* the Court identified the policy concerns raised by the defendant as a difficult issue and considered the analysis in *Ari* that supported the defendant's position. However, it concluded that the indeterminate liability concerns that arose in *Ari* did not apply because the same duty is not legislated for all private entities (at para 132). The indeterminate liability concern is arguably greater in the case at hand, in that the duty of care that the Plaintiff seeks to impose could

potentially apply to any public entity storing personal or confidential information through an online portal.

[115] In *Ari* and other authorities upon which the Defendant relies, courts have been prepared to conclude at the pleadings or certification stage of a proceeding that, based on policy considerations, including concerns of indeterminate liability, no duty of care exists. *Ari* expressly stated that this determination did not require consideration at trial of the factual matrix beyond that disclosed in the pleadings (at para 63). However, *Ari* is distinguishable on this point, because the indeterminate liability concern resulted from the fact that the source of the duty alleged by the plaintiff arose solely out of ISBC's statutory obligation under the *Freedom of Information and Protection of Privacy Act*, RSBC 1996, c 165, to make reasonable security arrangements to protect personal information in its custody. The Court reasoned that every public body collecting personal information could be subject to the same private law duty of care that the plaintiff sought to impose based on the statutory obligation (at para 50).

[116] In contrast, in the case at hand, the Plaintiff emphasizes that he is proposing a Class composed of only those persons who established a relationship with the Government by registering for online portals that store personal and financial information, giving rise to what he argues is a duty by the Government to secure those portals reasonably. The factual matrix available on the pleadings does not allow the Court to assess the breadth of the Government's practice of employing such portals. While it remains available to the Defendant to advance its public policy arguments at trial based on an evidentiary record, I am not presently able to

conclude, based on the Defendant's indeterminate liability argument, that it is plain and obvious that the Plaintiff has not disclosed a viable cause of action in systemic negligence.

(b) *Breach of Confidence*

[117] To succeed in a claim for breach of confidence, a plaintiff must prove: (a) that the plaintiff conveyed confidential information to the defendant; (b) that the information was conveyed in confidence; and (c) that the defendant then misused the information to the plaintiff's detriment (see *Lac Minerals Ltd v International Corona Resources Ltd*, [1989] 2 SCR 574). The Defendant submits that the Plaintiff's pleadings fail to disclose a reasonable cause of action for breach of confidence, both because they do not set out material facts necessary to establish the requirement of misuse and because the Defendant's failure to prevent the relevant cyber attacks does not represent misuse within the meaning of this tort. The Defendant therefore argues that the breach of confidence claim is doomed to fail.

[118] The Third SOC contains only one paragraph under the "Breach of Confidence" heading, which alleges that the personal financial information in the online Government accounts of the Plaintiff and other Class Members was confidential, was communicated to the Defendant in confidence, and was misused by the Defendant. I agree with the Defendant's submission that, in relation to the requirement of misuse, this paragraph represents bald assertions and does not allege material facts necessary to support a cause of action (see *Jensen v Samsung Electronics Co Ltd*, 2021 FC 1185 [*Jensen*] at para 77).

[119] However, performing the required review of the pleading as a whole (see *Mancuso v. Canada (National Health and Welfare)*, 2015 FCA 227 at para 18) reveals more detail of the Plaintiff's allegation of misuse underlying the breach of confidence claim, which relies on essentially the same factual basis as his claim in systemic negligence. In the "Background" section of the Third SOC, the Plaintiff alleges that the Defendant knew or ought to have known that its databases and online systems were vulnerable to data breaches; that it failed to take timely, reasonable and adequate measures to protect the information in its databases; that it failed to follow its own cybersecurity guidance regarding passwords; that it should have offered a non-vulnerable security question mechanism; and that it should have followed industry norms regarding two factor authentication.

[120] In my view, the Plaintiff's pleading is sufficient to perform its role of identifying the issues for the Defendant (see *Jensen* at para 77). However, turning to the Defendant's second argument, that its failure to prevent the cyber attacks does not represent misuse within the meaning of the breach of confidence tort, in my view, there is jurisprudential support for the Defendant's position.

[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 cyber attack 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.

(c) *Intrusion upon Seclusion*

[125] The tort of intrusion upon seclusion, as recognized by the Court of Appeal for Ontario in *Jones v Tsige*, 2012 ONCA 32 [*Tsige*], involves the following elements: (a) the defendant's conduct must be intentional or reckless; (b) the defendant must have invaded, without lawful justification, the plaintiff's private affairs or concerns; and (c) the invasion must be such that a reasonable person would regard it as highly offensive, causing distress, humiliation or anguish (at para 71). As with the breach confidence tort, the Defendant argues that there is no viable cause of action for intrusion arising from a database breach, where the bad actor is a third party,

not the defendant that maintained the database. Essentially, the Defendant's position is that this tort can be advanced only against an intruder and, in the case at hand, it is the threat actor and not the Defendant, which is the intruder.

[126] Again, there is jurisprudential support for the Defendant's position, found in recent authorities from the Ontario Superior Court of Justice. In *Owsianik v Equifax Canada Co,* 2021 ONSC 4112 [*Owsianik*], the Divisional Court held that the tort of intrusion upon seclusion has nothing to do with a database defendant. The Court held that to extend liability under this tort to a person who does not intrude, but rather fails to prevent the intrusion of another, would represent more than an incremental change to the common law (at para 54).

[127] *Owsianik* has been followed in other Ontario decisions. For instance, in *Del Giudice,* the Court declined to certify a claim for intrusion upon seclusion. It explained that Ms. Thompson was the intruder and that, while Capital One and Amazon Web were alleged to have increased the risk of data breach or to have failed to prevent the breach, a failure to prevent intrusion, even if reckless, was not intrusion (at para 136). This recent Ontario jurisprudence is very much on point in favouring the Defendant's position.

[128] However, the Plaintiff emphasizes that there are also authorities that diverge from that position. In *Kaplan,* the Ontario Superior Court of Justice reasoned that intrusion upon seclusion 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 a hacker's invasion. As such, the Court was not prepared to say that the intrusion claim was plainly

and obviously doomed to fail (at para 29). *Kaplan* relied in part on *Tucci*, in which the Supreme Court of British Columbia held that, while it was a stretch to say that the defendant invaded the plaintiff's private affairs, as that was done by a third party, it was not plain and obvious that being sufficiently reckless may not result in that conduct being attributed to the defendant. The Court concluded that intrusion upon seclusion was a relatively new tort and should be allowed to develop through full decisions (at para 152).

[129] Ultimately, *Tucci* declined to certify this tort under British Columbia common law because of binding authority based on the fact that British Columbia already has an intentional privacy tort in its provincial legislation. While *Tucci* certified the tort under federal common law, the Court of Appeal for British Columbia concluded that it was an error to conceive of federal and provincial common law being separate bodies of legal principles (see *Tucci BCCA* at paras 69-90). However, the Plaintiff notes that *Tucci BCCA* also observed that it was unfortunate that no appeal had been taken from the decision not to certify the tort under provincial law and expressed the view that the time may well have come for the Court to revisit its jurisprudence on the tort of breach of privacy (at para 55).

[130] It is difficult to read much into this observation in *Tucci BCCA.* However, I take the Plaintiff's point that a reasonable argument can be made that the jurisprudence on the potential scope of the tort of intrusion upon seclusion is not entirely settled. It is also useful again to consider the approach of the Federal Courts in *Condon* and *John Doe* and the related appeal decisions. In *Condon*, the Federal Court found that it was not plain and obvious that an action based on the tort of intrusion upon seclusion would fail (at para 64), rejecting the argument that

the plaintiffs did not allege that the defendant invaded their private affairs without justification. The Court held that the plaintiffs had sufficiently responded to this argument by pleading that their personal information was disclosed in an unlawful way (at para 54-58). While *Condon FCA* did not interfere with this conclusion, it does not appear that this issue was raised on appeal.

[131] In *John Doe*, the Federal Court held that the pleading of this tort was sufficient, that the area of privacy rights was developing rapidly, and that this tort's development or limitation should not be decided at the certification stage of the litigation (at paras 39-40). However, the Federal Court of Appeal disagreed, finding that it was plain and obvious that this cause of action could not possibly succeed. It reasoned that, at best, the pleadings supported that an isolated administrative error was made and concluded that there were no material facts pleaded to support an allegation of bad faith or recklessness (*John Doe FCA* at para 58).

[132] I find the present case distinguishable from *John Doe FCA*, on the basis that the Plaintiff has expressly pleaded recklessness on the part of the Defendant in ignoring reports by Class Members and service providers such as accounting and investment firms of unauthorized data breaches of Class Members' online Government accounts. For purposes of the present analysis, I must assume these factual allegations to be true and would find they are sufficient to disclose a reasonable cause of action in intrusion by seclusion, if recklessness in failing to prevent a data breach by a third party is legally sufficient to support this tort. Whether such recklessness is indeed legally sufficient is the question which remains unsettled and, given that there is some potential support for the Plaintiff's position in the jurisprudence of the Federal Courts, I am unable to conclude that the Plaintiff's cause of action in intrusion by seclusion is bound to fail.

(3) Identifiable Class of Two or More Persons

[133] Rule 334.16(1)(b) requires the Court to consider whether there is some basis in fact to conclude there is an identifiable class of two or more persons. As previously noted, the evidence in this motion indicates that 48,110 CRA My Accounts were impacted by the unauthorized use of credentials, with 12,700 of those accounts showing evidence of being used for fraud. Similarly, the evidence indicates that 5,957 accounts across several Enabled Services of ESDC were potentially impacted by the data breach, including 3,200 compromised MSCAs that were used to access CRA My Accounts via the link between MSCA and CRA, 1,200 of which were used to apply for CERB or other COVID-related benefits. As such, there is clearly a basis in fact to conclude that the potential Class extends to two or more persons.

[134] The Rule 334.16(1)(b) requirement also entails identifying an appropriate definition for the proposed class. As explained by the Supreme Court in *Sun-Rype Products Ltd v Archer Daniels Midland Company*, 2013 SCC 58 at paragraph 57:

> 57. I agree with the courts that have found that the purpose of the class definition is to (i) identify those persons who have a potential claim for relief against the defendants; (ii) define the parameters of the lawsuit so as to identify those persons who are bound by its result; (iii) describe who is entitled to notice of the action (*Lau v. Bayview Landmark Inc.* (1999), 40 C.P.C. (4th) 301 (Ont. S.C.J.), at paras. 26 and 30; *Bywater v. Toronto Transit Commission* (1998), 27 C.P.C. (4th) 172 (Ont. Ct. J. (Gen. Div.)), at para. 10; Eizenga et al., at § 3.31). *Dutton* states that "[i]t is necessary . . . that any particular person's claim to membership in the class be determinable by stated, objective criteria" (para. 38). According to Eizenga et al., "[t]he general principle is that the class must simply be defined in a way that will allow for a later determination of class membership" (§ 3.33).

[135] The class definition proposed by the Plaintiff is set out earlier in these Reasons. Leaving aside the definitions for the terms used therein, the substance of the definition reads as follows (with the underlined portion representing a change from the Third SOC to the Fourth SOC):

> All persons whose personal or financial information in their Government of Canada Online Account was disclosed to a third party <u>without authorization</u> on or after March 1, 2020, excluding Excluded Persons.

[136] The Defendant takes issue with the proposed definition on several bases. First, the Defendant submits that the definition is overly broad, and unrelated to the proposed common issues (which will be identified and addressed in more detail later in these Reasons), because it includes persons who had information in their accounts disclosed to a third party for any reason, even if unrelated to the conduct of the Defendant. This criticism is fair, particularly if one considers the definition set out in the Third SOC, in which the words "without authorization" are missing. As the Defendant submits, that definition would include disclosure to third parties that a Class Member had authorized, such as an accounting firm or other authorized representatives.

[137] However, it is clearly not the Plaintiff's intent to propose a Class that includes persons whose information was the subject of only authorized disclosure. This clarification is achieved through the inclusion of the words "without authorization" in the definition as set out in the draft Fourth SOC. Significantly, in my view, while the Fourth SOC was prepared as part of the Plaintiff's Reply Memorandum of Fact and Law filed on April 13, 2022, the Plaintiff's original Memorandum of Fact in Law dated December 10, 2021, also included these words. Notwithstanding the discrepancy between the definition proposed in the Memorandum of Fact

and Law and that contained in the Third SOC, in my view, the Plaintiff's intent is and has been clear from the definition included in his original Memorandum and from his overall submissions.

[138] In *Lin v Airbnb Inc*, 2019 FC 1563, Justice Gascon agreed with the defendant's objection to a proposed class definition, arguing that it was too broad, and was prepared to allow certification on condition that the class definition be amended (at paras 90-91). Although narrowing the class definition will require a pleading amendment, and notwithstanding the effect of the Case Management Order, I am satisfied that such an amendment is appropriate, and my Order will grant leave for that amendment.

[139] However, the amendment does not fully address the Defendant's position, which argues that the proposed Class definition would still capture persons whose information was disclosed without authorization as a result of a data breach not attributable to any conduct by the Defendant. For instance, as will be canvassed in more detail later these reasons, the Defendant takes the position that the Plaintiff himself was the victim of identity theft unrelated to the Defendant's conduct.

[140] While I accept the logic of the Defendant's submission, in my view it does not make the proposed Class definition inappropriate. As the Plaintiff argues, the definition is intended to be objective rather than merits-based, notwithstanding that this may result in it being over-inclusive (see, e.g. *Tiboni v Merck Frosst Canada Ltd*, 2008 CanLII 37911 (ONSC) at para 64-82). The objective nature of the definition results from the Class Members being able to identify as having

been subject to data breaches within the relevant temporal limits, based on the notices sent by the Government or their own observations of unauthorized activity in their online accounts.

[141] The Defendant also takes issue with the temporal limits, or lack thereof, of the Plaintiff's proposed definition. The Plaintiff submits that the definition should capture unauthorized disclosures beginning as of March 1, 2020. He has not proposed any end date for the definition. In support of these positions, the Plaintiff argues that, while the evidence is that the bulk of the cyber incidents occurred between June and August 2020, the timing of commencement of the data breaches is not yet known. As I understand the Plaintiff's reasoning behind the proposed commencement date, it is intended to shortly precede the first of the CERB application periods, which commenced on March 15, 2020. Given the evidence that the cyber incidents were motivated by interest on the part of the threat actors in exploiting CERB and other COVID-related benefits, I accept that there is some basis in fact for the March 1, 2020 commencement date in the definition proposed by the Plaintiff.

[142] However, I agree with the Defendant's position that it is appropriate that the definition include an end date, selected by reference to evidence as to when the deficiencies in the Defendant's system as alleged by the Plaintiff were addressed. The Defendant suggests a date in August 2020. The Plaintiff argues that this is too early, as some of the Defendant's remedies were not implemented until later in 2020.

[143] While I appreciate the evidence that the Defendant's first interventions in response to the data breach occurred in August 2020, I also note the evidence in the Defendant's expert report of

Christopher McDonald that CRA began to add multifactor authentication to My Accounts in September and October 2020 and that ESDC added this protection in December 2020. I rely on this evidence as a basis in fact to conclude that the Proposed Class definition should include an end date of December 31, 2020.

(4) Common Questions of Law or Fact

[144] The next requirement, prescribed by Rule 334.16(1)(c), is that the Plaintiff demonstrate some basis in fact for the claims of the class members raising common questions of law or fact, regardless of whether those common questions predominate over questions affecting only individual members. I have listed earlier in these Reasons the common questions proposed by the Plaintiff and will now address the parties' respective submissions on whether the Plaintiff has demonstrated some basis in fact for these questions.

(a) *Systemic Negligence*

[145] The Plaintiff submits that the evidence establishes a basis in fact to conclude that the Class Members' claims raise common questions surrounding the elements of a cause of action in systemic negligence, i.e. whether the Defendant owed the Class a duty of care, identification of the applicable standard of care, whether the Defendant breached that duty, and whether that breach caused damages to the Class.

[146] In relation to all these questions, the Defendant takes the position that their answers would turn on Class Members' individual circumstances and are therefore ill-suited for

determination on a class-wide basis. In relation to the duty and standard of care, the Defendant submits that both will depend on the particular nature of the information that exists in a particular online Government account, as well as the reason that information has been collected, which will vary significantly among different types of accounts. By way of example, the Defendant argues that the standard of care applicable to CRA collecting taxpayer information cannot be the same as for Parks Canada collecting a name and address for a campsite reservation.

[147] The Defendant refers the Court to *Kaplan*, in which an anonymous hacker accessed a casino's computer system, stole personal information relating to customers, employees and suppliers, and posted it online. The Court refused to certify the duty and standard of care questions, because the type and amount of personal information accessed by the hacker in that case varied widely between individuals (at para 64). It accepted that, if an issue can be resolved only by asking it of each class member, it is not a common issue (at para 55).

[148] In support of its position that this reasoning applies to the case at hand, the Defendant submits that the GCKey service is used by over 30 government departments and agencies to access multiple governmental online Enabled Services that collect only mundane information. The Defendant also relies on the evidence that, in the case of some of the online Government accounts that were impacted by the cyber incidents, the level of intrusion was minimal, such as accessing only the CRA My Account homepage. The Defendant contrasts these circumstances with those in *Condon* and *John Doe*, in which the information collected, stored and allegedly disclosed was the of the same nature for each class member.

[149] The Defendant advances similar arguments in relation to the proposed common question as to whether the Defendant's alleged breach of duty caused damage to the Class. The Defendant notes that there is difficulty in working backward from alleged fraud experienced by an individual and attributing it to a specific data breach, because fraud and cyber attacks are common in today's online world. Therefore, the Defendant submits that causation cannot be assessed without an examination of the specific circumstances of each individual Class Member, including consideration of whether contributory negligence may be attributed to a particular Class Member, for instance as a result of the imprudent reuse of credentials.

[150] I accept that not all online Government accounts that were accessed in the data breaches would necessarily have contained sensitive information, and I accept that some Class Members' accounts suffered a higher level of intrusion than others. The points raised by the Defendant that may require consideration in connection with causation, including contributory negligence, are also valid. However, I agree with the Plaintiff's position that these potential differences among Class Members' claims are not necessarily an impediment to certification. As the Supreme Court explained in *Vivendi Canada Inc v Dell'Aniello*, 2014 SCC 1 [*Vivendi*] at paragraphs 44 to 46:

> 44. In *Rumley v. British Columbia*, 2001 SCC 69, [2001] 3 S.C.R. 184, this Court confirmed the principles from *Dutton*. In the case of the commonality requirement, the purpose of the analysis is to determine "whether allowing the suit to proceed as a representative one will avoid duplication of fact-finding or legal analysis": para. 29, quoting *Dutton*, at para. 39. The Court also stated that a question can remain common even though the answer to the question could be nuanced to reflect individual claims: para. 32.
>
> 45. Having regard to the clarifications provided in *Rumley*, it should be noted that the common success requirement identified in *Dutton* must not be applied inflexibly. A common question can exist even if the answer given to the question might vary from one member of the class to another. Thus, for a question to be

> common, success for one member of the class does not necessarily have to lead to success for all the members. However, success for one member must not result in failure for another.
>
> 46. *Dutton* and *Rumley* therefore establish the principle that a question will be considered common if it can serve to advance the resolution of every class member's claim. As a result, the common question may require nuanced and varied answers based on the situations of individual members. The commonality requirement does not mean that an identical answer is necessary for all the members of the class, or even that the answer must benefit each of them to the same extent. It is enough that the answer to the question does not give rise to conflicting interests among the members.

[151] To similar effect, in *Campbell v Flexwatt Corp*, 1997 CanLII 4111 at paragraph 53, the British Columbia Court of Appeal observed that common issues do not have to be issues, which are determinative of liability. They need only be issues of fact or law that move the litigation forward. In class proceedings in the Federal Court, Rule 334.26 provides for procedural mechanisms for the determination of any individual issues that remain following a judgment on common questions of law or fact.

[152] The Defendant responds to these submissions by arguing that *Vivendi* was not a systemic negligence case. I am not persuaded by that argument, as I read the principles from *Vivendi* upon which the Plaintiff relies to be of general application. Applying those principles, I find compelling the Plaintiff's submission that the variation in the types of accounts and information that were breached is dwarfed by the commonality, in the sense that all persons whose accounts were breached registered for online accounts, and there is commonality in the alleged flaws that the Plaintiff says permitted the breaches: including requiring insufficiently robust passwords, misconfiguration of the security question protocol, and a lack of two factor authentication.

[153] Moreover, I do not regard this as a case akin to *Kaplan*, in which it can be concluded that each Class Member's claim must be analysed individually in order to answer the questions surrounding duty and standard of care or causation. By way of example only, if it were to be assumed that there are variations in the level of sensitivity of the information maintained in the online portals of the over 30 Government departments that the evidence indicates rely upon the GCKey service (as well as further variations over different Enabled Services), these variations might result in a significant number of nuanced responses to the common questions. However, this process would still serve to move the litigation forward. Moreover, to the extent particular Class Members' claims may raise unique issues individual to them, including contributory negligence, the Court is equipped to address these at the individual stage of the litigation.

[154] The Defendant also argues that the Plaintiff has presented no basis in fact for the certification of Class Members' damages as a common issue. The Defendant submits that the damages will need to be determined on an individual basis. It notes that the unauthorized disclosure of any individual Class Member's information may not actually lead to anxiety, future identity theft, or any of the other claimed heads of damages, particularly in the case of those who had only mundane information disclosed. In response to these arguments, the Plaintiff repeats its submissions above on the application of the principles derived from *Vivendi*. For the reasons explained above, I find those submissions compelling.

[155] However, the Defendant also takes the position that some Class Members may have no basis to claim damages at all, as applicable jurisprudence explains that damages for stress and anxiety may be compensated only when they are serious and prolonged and rise above life's

ordinary annoyances, anxieties and fears (see *Saadati v Moorhead*, 2017 SCC 28 [*Saadati*] at para 37; *Mustapha v Culligan of Canada Ltd*, 2008 SCC 27 [*Mustapha*] at para 9).

[156] Moreover, the Defendant argues that, with the exception of the claim for anxiety, each of the claimed heads of damages constitutes a pure economic loss claim, which is not compensable in negligence except in limited circumstances that do not apply. The Defendant refers the Court to *Del Giudice*, which concluded that the majority of the class members' anxiety claims would not rise to the level of compensable harm and that the remaining claims were for non-compensable pure economic loss (at paras 223-228).

[157] In response, the Plaintiff argues that *Saadati* has advanced the jurisprudence surrounding claims for mental injury in a manner that favours his position. While the Plaintiff accepts that Class Members would be required to demonstrate mental disturbance that is serious and prolonged and rises above the ordinary annoyances, anxieties and fears that come with living in a civil society, he emphasizes the Supreme Court's recognition that claimants need not demonstrate that their mental injury is classified as a recognized psychiatric illness (at para 37). This development was explained in *Reddock v Canada (Attorney General)*, 2019 ONSC 5053 (appeal allowed 2020 ONCA 184 on other grounds), which also identified that it is therefore not necessary to rely on expert opinion in order to establish a compensable mental injury (at paras 387-390).

[158] The Plaintiff also refers to the Court to other post-*Saadati* cases (including *Condon FCA* and *John Doe FCA*) that have certified claims relating to mental distress and inconvenience in

the breach of privacy context. In particular, in *Condon FCA*, the Federal Court of Appeal overturned the Federal Court's decision not to certify causes of action in negligence and breach of confidence because of a lack of compensable damages.

[159] In *Condon*, the Federal Court identified that the plaintiffs' negligence and breach of confidence claims sought damages for wasted time, inconvenience, frustration, anxiety and increased risk of future identity theft, resulting from the data loss (at para 66). However, the Court found, based on the evidence adduced, that the plaintiffs had not suffered any compensable damages, as they had not been victims of fraud or identity theft, had spent minimal time seeking status updates from the relevant Minister, and did not avail themselves of any credit monitoring or other services offered by the defendant (at para 68). Relying in part on *Mustapha*, the Court concluded that damages are rarely awarded for mild disruption alone and held that it was plain and obvious that the claims based on negligence and breach of confidence would fail for lack of compensable damages (at paras 73-79).

[160] On appeal, *Condon FCA* held that this evaluation of the evidence represented an error, as the Federal Court should have determined whether the plaintiffs had a reasonable cause of action based on the facts as pled (including costs incurred in preventing identity theft and out-of-pocket expenses) rather than the evidence (at paras 5, 14-22).

[161] In *John Doe FCA*, the Federal Court of Appeal relied on *Condon FCA* in concluding that the Federal Court in *John Doe* had not erred in finding that the plaintiff's pleading in negligence and breach of confidence was sufficient, based on their identification of the nature of the

damages claimed. In addition to claims for mental distress as well as inconvenience, frustration and anxiety associated with precautionary steps taken to prevent home invasion, theft, robbery and/or damage to personal property, the pleading sought costs related to such steps. The Court of Appeal concluded that such costs were not negligible inconveniences or entirely speculative and noted that it was to be assumed that the claimed costs had been incurred in light of the principle that a statement of claim is to be read as generously as possible at the certification stage of the class action (at paras 49-51).

[162] In considering the application of *Condon FCA* and *John Doe FCA* to the present issue, I note first that both decisions addressed the Rule 334.16(1)(a) requirement that the pleadings disclose a reasonable cause of action, not the Rule 334.16(1)(c) requirement that the claims of the class members raise common questions of law or fact. As explained earlier in these Reasons, when considering the Rule 334.16(1)(c) requirement, the Court must consider the evidence adduced on the certification motion. I nevertheless find these authorities instructive in resolving the parties' disagreement on whether the evidence demonstrates a basis in fact for the Class Members' damages claim. These authorities support a conclusion that defence arguments based on the principles in *Saadati/Mustapha*, or related to the recoverability of pure economic loss, are best addressed in considering the sufficiency of pleadings in demonstrating a viable cause of action. Moreover, these authorities support a conclusion that, in a breach of privacy case, it is not plain and obvious that a plaintiff will fail in asserting a claim for categories of damages such as mental stress and anxiety or out-of-pocket expenses related to the risk of identity theft.

[163] Of course, the Plaintiff must still adduce evidence supporting some basis in fact for the Court to conclude that the Class Members' claims raise a common question related to the damages claimed. I find this requirement satisfied by the evidence of the Plaintiff and other of the Plaintiff's affiants, identifying steps taken and costs incurred as a result of the data breaches, as well as mental harm they say they have suffered. It will remain available for the Defendant to raise pure economic loss and *Saadati/Mustapha* arguments in a common issues trial. However, for purposes of this motion, I am satisfied that the low threshold represented by some basis in fact has been met.

[164] In so concluding, I am conscious that, other than the Plaintiff, the other affiants represent "Excluded Persons" within the meaning of the Class definition, and therefore will not actually be Class Members. Their affidavits were prepared before the amendment to the proposed Class resulting from the Murphy Battista data breach. However, I accept the Plaintiff's argument that their evidence is nevertheless indicative of the categories of damages incurred by those affected by the cyber incidents at issue in this action who would fall within the Class definition.

[165] I have also considered the Defendant's argument, in relation to the Plaintiff in particular, that he admitted on cross-examination that the anxiety he experienced in the summer of 2020 was largely due to a traumatic incident unrelated to the cyber breaches. I agree with the Plaintiff's response that a tortious act need not be the sole cause of injury in order to be actionable (see *Athey v Leonati*, [1996] 3 SCR 488 at para 17). The Plaintiff's affidavit evidence that he has experienced significant anxiety and stress as a consequence of the breach of his CRA

account provides some basis in fact for this aspect of the damages claim that he seeks to pursue in common with other Class Members.

(b) *Breach of Confidence*

[166] The Plaintiff submits that the evidence establishes a basis in fact to conclude that the Class Members' claims raise a common question whether the Defendant is liable to them for the tort of breach of confidence. The Defendant disagrees, but has offered no particular submissions in support of this position other than those analysed earlier in these Reasons in connection with the viability of this cause of action under Rule 334.16(1)(a).

[167] As with the systemic negligence claim, the Plaintiff argues that the focus of the claim for breach of confidence is on the Defendant's overall conduct and implementation of policy, rather than on the individual circumstances of the Class Members. Based on the same evidence on which the Plaintiff relies for certification of the common questions related to systemic negligence, I find that the evidence raises some basis in fact for the proposed question related to breach of confidence.

(c) *Intrusion upon Seclusion*

[168] Similarly, the Plaintiff submits that the evidence establishes a basis in fact to conclude that the Class Members' claims raise a common question whether the Defendant is liable to them for the tort of intrusion upon seclusion. The Defendant responds that there is no evidence

provided, by way of affidavit or otherwise, that the Defendant, as opposed to the threat actor, invaded the Class Members' privacy or that the Plaintiff or any Class Member was humiliated.

[169] On the latter point, *Tsige* explains that one of the elements of intrusion upon seclusion is that the invasion must be such that a reasonable person would regard it as highly offensive, causing distress, humiliation or anguish (at para 71). As noted in *Condon*, the focus is upon what a reasonable person would conclude would result from the intrusion, not whether the information at issue actually caused humiliation. Moreover, frustration and anxiety could represent forms of distress (at paras 60-61). I do not find the absence of Class Members expressly deposing to being humiliated a compelling argument.

[170] The argument that there is no evidence that the Defendant, as opposed to the threat actor, intruded upon the Class Members' privacy merely repeats the Defendant's argument that failure to protect against intrusion by a third party is insufficient to support this cause of action. I addressed this argument earlier in these Reasons.

[171] Finally, the Defendant submits that the determination of whether the relevant intrusion would be highly offensive to a reasonable person cannot be decided in this case on a class-wide or common basis, given the disparate types of information at issue. Again, as reasoned in the context of the proposed systemic negligence questions, I find the Plaintiff's arguments based on *Vivendi* responsive to this submission.

[172] The Plaintiff relies upon the same evidence that supports certification of the common questions related to systemic negligence and breach of confidence, arguing that the Defendant's conduct represents the recklessness necessary to support the tort of intrusion upon seclusion. I find that this evidence raises some basis in fact for the proposed question related to that tort.

(d) *Aggregate Damages*

[173] The Plaintiff's proposed common question on aggregate damages asks whether the Court can make an aggregate assessment of all or part of the damages suffered by Class Members and, if so, in what amount.

[174] The Defendant opposes certification of this question, referencing the explanation in *Paradis Honey Ltd v Canada (Agriculture and Agri-Food)*, 2018 FC 814 [*Paradis Honey*] at paragraph 27, that aggregate assessment is not the tallying of the individual class members' claims but rather is a communal assessment of the totality of the claims where the underlying facts permit such an assessment to be done with reasonable accuracy. The Defendant submits there is no common amount that objectively could be awarded to every Class Member, because not every proposed Class Member's information was actually disclosed causing harm, some Class Members had mundane information disclosed that may not be worthy of compensation, and others that information disclosed that was already in the public domain.

[175] The Defendant also relies on *McCrea* at paragraph 377, in which the Court declined to certify a question whether general damages could be determined on an aggregate basis, agreeing with the defendant in that case that individual assessment would be required. However, the Court

in *McCrea* explained that the plaintiff had not proposed any methodology for the determination of aggregate damages. As will be canvassed below, the Plaintiff in the case at hand has proposed such a methodology through the Allen Report.

[176] Moreover, while I note the explanation in *Paradis Honey* as to the nature of aggregate damages, I do not find the decision in that case to support the Defendant's position. That decision addressed a motion by the defendant for documentary production by the plaintiffs following certification of the class action in that matter, including certification of the question whether aggregate damages were available. The plaintiffs refused to produce documents including their personal financial records on the grounds that they were not relevant to the common issues. In rejecting that position and ordering the requested production, the Court reasoned that, in order to consider the damages claimed and determine how such damages might be calculated in the aggregate or otherwise, it was necessary to consider a particular plaintiff's circumstances, as well as how such circumstances might differ between plaintiffs in the class action (at paras 27-30).

[177] As explained in more detail earlier in these Reasons, the Plaintiff offers the Allen Report as expert evidence of two methodologies that could be used to calculate aggregate damages in this matter. As also previously explained, the Defendant takes issue with Dr. Allen's opinions and relies on the PWC Report in support of its positions, arguing that the Allen Report should be afforded little weight. However, it is not the Court's role in a certification motion to engage in detail with the parties' respective expert opinions and address disputes therein. It is sufficient at this stage that Dr. Allen's opinions raise some basis in fact for a conclusion that there are

methodologies that could be used to calculate damages on an aggregate basis. I am therefore satisfied that this proposed question should be certified.

(e) *Punitive Damages*

[178] The Plaintiff's proposed common question on punitive damages asks whether the conduct of the Defendant merits an award of punitive damages and, if so, in what amount.

[179] The Defendant opposes certification of this question on the basis that the Plaintiff does not allege malice on the part of the Defendant or plead any facts to support a basis for awarding punitive damages. As the Defendant submits, punitive damages are awarded only in exceptional circumstances for high-handed, malicious, arbitrary or highly reprehensible misconduct that departs to a marked degree from ordinary standards of decent behaviour (see *Whiten v Pilot Insurance Co*, 2002 SCC 18 at para 94).

[180] The Plaintiff has provided little in the way of submissions in support of this proposed question. Indeed, at the hearing of this motion, the Plaintiff's counsel brought to the Court's attention the recent decision in *MacKinnon v Pfizer Canada Inc*, 2022 BCCA 151, in which the British Columbia Court of Appeal concluded that the motions judge erred in certifying a proposed common issue on punitive damages solely on the basis of the allegations in the pleadings. As the plaintiffs had not pointed to any material beyond the pleadings to establish a basis in fact for the certification of this common issue, the certification of the punitive damages issue was set aside.

[181] Similarly, in the case at hand, the Plaintiff has not referred to Court to any evidence on which he relies as some basis in fact to certify a common question related to punitive damages. I therefore find that it would be inappropriate to certify this question.

(5) Preferable Procedure

[182] The next requirement is that a class proceeding be the preferable procedure for the just and efficient resolution of the common questions. In assessing this requirement, the Court must consider all relevant matters, including those expressly set out in Rule 334.16(2), which in turn include whether the common questions predominate over any questions affecting only individual class members.

[183] The Defendant's submissions on this issue focus on its argument that individual issues surrounding liability, injury, causation, and damages, specific to each individual claimant, predominate over the common issues. I accept that, as expressly contemplated by Rule 334.16(2)(a), whether common or individual issues predominate is a factor to be considered in assessing whether there is a procedure that is preferable to a class action. As the Defendant submits, a class action may be found not to be the preferable procedure based on the need for individual proof by class members (see, e.g., *Setoguchi v Uber BV*, 2021 ABQB 18 at para 97).

[184] However, as the Plaintiff argues, the preferability inquiry is to be conducted through the lens of the three principal goals of class actions, namely judicial economy, behaviour modification and access to justice. This does not represent a requirement to prove that the proposed class action will actually achieve those goals in the specific case. Rather, the

preferability analysis is a comparative exercise. While the Court must consider whether the proposed class action will achieve these goals, the ultimate question is whether other available means of resolving the claim are preferable if a class action would not fully achieve these goals (see *AIC Limited v. Fischer*, 2013 SCC 69 at paras 22-23).

[185] As such, I agree with the Plaintiff's position that the difficulty with the Defendant's arguments is that they assert that a class action is not the preferable procedure but offer no alternative. In the absence of a class action, the only apparent option for claimants who would otherwise be Class Members would be to bring individual actions against the Defendant. Based on the nature of the damages claimed, I agree with the Plaintiff's argument that such actions would likely be uneconomic, effectively leaving claimants with no alternative at all.

[186] In my view, the Plaintiff's action meets the goals that animate class proceedings. Access to justice is achieved in circumstances where such access would otherwise likely be unavailable due to the applicable economics. Judicial economy is achieved, because there are at least some aspects of the litigation that can be advanced in common and therefore will not require repetition multiple times. By way of example, evidence surrounding the Defendant's policies, practices, and the manner in which the 2020 cyber incidents occurred can be adduced only once rather than potentially thousands of times.

[187] With respect to the goal of behaviour modification, the Defendant submits that it followed all appropriate steps once it learned it was the victim of a breach and that behaviour modification therefore has no application. I agree with the Plaintiff's response to this argument.

Behaviour modification is intended to prevent breaches from occurring in the first place, by creating the motivation to take proactive steps to avoid such events.

[188] I am satisfied there is a basis in fact to conclude that a class proceeding is the preferable procedure for the just and efficient resolution of the common questions in this matter.

(6) Representative Plaintiff

[189] The final requirement for certification is that there is a representative plaintiff who meets certain conditions prescribed by Rule 334.16(1)(e), including that they would fairly and adequately represent the interests of the class (Rule 334.16(1)(e)(i)) and have prepared a plan for the proceeding that sets out a workable method of advancing the proceeding on behalf of the class and of notifying class members as to how the proceeding is progressing (Rule 334.16(1)(e)(ii)).

[190] The Defendant takes the position that the Plaintiff is not an appropriate representative, arguing that he does not have a basis for a claim against the Defendant and that his claim is not representative of the claims of the proposed Class Members.

[191] In addition to the Rae Affidavit referenced earlier in these Reasons, Mr. Rae affirmed a second affidavit dated February 14, 2022, in response to the November 25, 2021 affidavit of the Plaintiff, Mr. Sweet, after he was proposed as the new representative plaintiff. Mr. Rae explains in his second affidavit activity that occurred in the Plaintiff's CRA My Account in June, July and August 2020. This includes the Plaintiff's account being accessed on June 29, 2020, using a valid

username and password, without any signs of brute force attack or password guessing, as well as a correct answer to the randomly selected security question after only one failed attempt. The user accessing the account then modified the security questions and answers, likely to maintain persistent access to the account, deleted the email address on file, changed the direct deposit information, and applied for four periods of CERB.

[192] Mr. Gad also affirmed a second affidavit, dated February 11, 2022, again in response to the Plaintiff's affidavit. Mr. Gad explains that he reviewed the security logs of the Plaintiff's CRA My Account from June 15 to August 15, 2020, and found no signs of bot activities used to gain access to this account and no signs of credential stuffing attack techniques. Mr. Gad found that the username and password for the Plaintiff's account were entered correctly for each access attempt and that there were no signs of password guessing.

[193] Mr. Gad also explains that the CRA IT Security team was able to locate the Plaintiff's combination of username and password on the Dark Web as part of a third party data breach that occurred in 2018. Finally, he explains that the CRA IT Security team flagged the Plaintiff's account for unauthorized activities based on an attempt to access the account on July 22, 2020, using the security question bypass method, following use of the correct username and password to login. However, the account was already locked at that point, and the user was not able to access the account.

[194] I understand the Defendant to take the position that this evidence indicates that the Plaintiff was the victim of identity theft unrelated to the Defendant's conduct impugned in this

action. While the Defendant may be able to rely on this evidence at a future stage in the proceeding in an effort to argue either that the Defendant is not liable to the Plaintiff or that there are aspects of other Class Members' claims which differ from those of the Plaintiff, I am not convinced that these arguments make the Plaintiff an unsuitable representative. Certainly, the Court considering a certification motion is not expected to enter into any merits based assessment of the proposed representative plaintiff's individual claim (see *TL v Alberta (Director of Child Welfare)*, 2006 ABQB 104 at paras 117).

[195] As I read the authorities cited by the Defendant (*Canada (Attorney General) v Jost*, 2020 FCA 212 at paras 103-105, and *Fehr v Life Assurance Company of Canada*, 2015 ONSC 6931 at para 335), they focus principally on the requirement that the representative plaintiff is actually a member of the class (see also *Piett v Global Learning Group Inc*, 2021 SKQB 232 at paras 69-72). As explained in *Williamson v Johnson & Johnson*, 2020 BCSC 1746 [*Williamson*], it is possible to find that the representative plaintiff will adequately and fairly represent the class, even where there are differences, as long as there is no impact on the common issues. The Court in *Williamson* noted such potential differences and reasoned that, as a result, the proposed representatives may advocate vigorously for a broad basis of liability on the part of the defendant (at paras 339-342).

[196] There is clearly a basis in fact, relying even on the Defendant's evidence, to conclude that the Plaintiff's CRA My Account was accessed without authorization in the summer of 2020 and that he therefore falls within the Class definition. To the extent there may be differences, as between the Plaintiff and other Class Members, as to the circumstances under which an account

was breached or the mechanisms employed to accomplish such breach, I am not convinced that such differences would undermine the Plaintiff's ability or motivation to fairly and adequately represent the interests of the Class.

[197] The Defendant also argues that the Plaintiff's litigation plan filed in support of this motion fails to address key matters, including a plan to determine who is a Class Member, the presence of individual issues, and an acceptable method for addressing such issues. The Defendant argues in particular that nothing in the Plaintiff's material suggests that he has considered whether any individual Class Member could prove causation. The Defendant also relies on the Plaintiff's cross-examination as indicating that the litigation plan in the motion materials is outdated and fails to include important information. The Plaintiff also acknowledged in cross-examination that there are significant aspects about the prosecution of the case about which he knows nothing.

[198] I agree with the Defendant that the Plaintiff's litigation plan is light. It is relatively generic and does not engage in any substantive way with the potential need to address common questions in a nuanced manner or otherwise address the potential individual issues upon which many of the Defendant's arguments focus. The plan is also clearly outdated, as it relies to some extent on the experience and resources of Murphy Battista, who are no longer involved.

[199] However, I am not convinced that the plan is so inadequate that the Court should decline to certify this proceeding. In *Mackinnon v Pfizer Canada Inc*, 2021 BCSC 1093 (affirmed 2022

BCCA 151 other than in relation to certification of punitive damages), the Court addressed similar concerns as follows at paras 167-171:

> 167. Finally, the defendants say that the plaintiffs' proposed litigation plan is "rudimentary, vague and formulistic", and provides no insight into how the plaintiffs anticipate the common and individual issues will actually be resolved. The defendants take particular issue with the lack of detail as to how individual issues of causation and damages will be determined after a common issues trial.
>
> 168. The plaintiffs' litigation plan is relatively minimalist. It includes provision for notice to the class, examinations for discovery, document production, the exchange of expert reports, and the conduct of a common issues trial. The defendants are correct that there is limited detail regarding the individual trials that may follow the common issues trial. The litigation plan appears to depend on the exercise of the court's case management powers under the CPA.
>
> 169. The purpose of a litigation plan is to provide a framework for the class proceeding that shows that the representative and class counsel understand the complexities of the case. It is not intended to resolve all procedural issues before certification has occurred. It can be anticipated that litigation plans will require amendment as the case proceeds: *Jiang v. Vancouver City Savings Credit Union*, 2019 BCCA 149 at paras. 57—61 [*Jiang 2019*].
>
> 170. As observed by the Court of Appeal at para. 61 of *Jiang* 2019, ss. 12, 27 and 28 of the *CPA* provide post-certification tools to address how individual issues will be resolved. The adequacy of a litigation plan may be viewed through the lens of the case-management tools available to the court post-certification.
>
> 171. In my view, the plaintiffs' proposed litigation plan is sufficient at this stage of the proceeding to satisfy the requirement in s. 4(1)(e)(ii) of the *CPA*.

[200] Similarly, the Plaintiff's litigation plan in the case at hand addresses the principal steps that will be involved in progressing the litigation, including in some respects the method of providing notice to the Class, and relies significantly on the Court's case management to develop

more detailed approaches to addressing individual issues. As for the Plaintiff's acknowledgment that there are significant aspects about the prosecution of the case about which he knows nothing, I considered a similar argument in *Tippett*, concluding as follows at paragraph 88:

> 88. I accept that a number of the Plaintiff's responses to answers posed during his cross-examination demonstrate that he has little understanding of the litigation process. However, I do not consider this to disqualify him from being a representative plaintiff, when he has the benefit of competent counsel experienced in class action litigation. In *Pederson v Saskatchewan (Minister of Social Services)*, 2016 SKCA 142 at paras 95-106, the Saskatchewan Court of Appeal held that the certification judge erred in concluding that the proposed representative plaintiffs were unsuitable based on personal motivations and lack of understanding of the claim. The Court of Appeal noted that it is not surprising that litigants do not know the law or litigation procedures, as they look to competent counsel for advice in that respect. A detailed examination of the competence and circumstances of a proposed representative is not in accordance with the relatively low threshold for this requirement. Rather, a representative plaintiff should only be rejected where he or she clearly will not or cannot represent a class.

[201] Taking into account the relatively low threshold for the requirement in Rule 334.16(1)(e)(ii), I am satisfied that the Plaintiff's litigation plan, including intended reliance on future case management as this matter proceeds, represents a workable method of achieving the objectives set out in the Rule. Following certification, I will expect the parties to work together to develop a more detailed plan for identification of and notice to Class Members, including the time and manner in which they can opt out of the class proceeding, and present this plan to the Court through the case management process.

[202] Turning briefly to the other requirements in Rule 334.16(1)(e), nothing in the record indicates a conflict between the interests of the Plaintiff and those of other Class Members, and I

note that the Plaintiff's affidavit provides a copy of the contingency fee agreement that he has executed with his counsel. My conclusion is that the Rule 334.16(1)(e) requirements are satisfied.

V. **Conclusion**

[203] In conclusion, I find that the requirements for certification are met. The Order issued with these Reasons will address the points contemplated by Rule 334.17(1), in a manner consistent with the conclusions in these Reasons, subject to the reservation on the time and manner for class members to opt out of the class proceeding as mentioned above.

VI. **Costs**

[204] Pursuant to Rule 334.39, there are typically no costs awarded on a motion for certification. While the Defendant requested that the Plaintiff's motion for certification be dismissed with costs, the Plaintiff has not has sought costs, and I find no basis to award costs in granting this motion.

ORDER IN T-982-20

THIS COURT ORDERS that:

1. The Defendant's motion to strike certain paragraphs of the report dated December 11, 2020, of Dr. Douglas Allen is dismissed without costs.

2. The Defendant's motion to strike the affidavit of Elizabeth Emery dated July 23, 2021, is granted in part, and paragraph 2 and the related Exhibits B and C are stuck. The motion is otherwise dismissed, all without costs.

3. This action is hereby certified as a class proceeding.

4. Todd Sweet is appointed as the representative Plaintiff.

5. The definition of the class shall be as follows, and the Plaintiff is granted leave to amend his Statement of Claim to reflect this definition:

> All persons whose personal or financial information in their Government of Canada Online Account was disclosed to a third party without authorization between March 1, 2020, and December 31, 2020, excluding Excluded Persons.
>
> "Government of Canada Online Account" means:
>
> a. a Canada Revenue Agency account;
>
> b. a My Service Canada account; or
>
> c. another Government of Canada online account, where that account is accessed using the Government of Canada Branded Credential Service (GCKey).
>
> "Excluded Persons" means all persons who contacted Murphy Battista LLP about the CRA privacy breach class action, with Federal Court file number T-982-20 prior to June 24, 2021.

(Collectively “Class” or “Class Members”).

6. The nature of the claims made on behalf of the Class is as follows:

   The claims concern allegations that the Defendant was negligent and is also liable for intrusion upon seclusion and breach of confidence.

7. The relief claimed by the Class is as follows:

   The claims seek general and special damages, damages equal to the costs of administering notice and the plan of distribution, pre-judgment and post-judgment interest, and costs.

8. The following issues are certified as common questions of law or fact for the Class:

   Systemic Negligence

   A. Did the Defendant owe the Class a duty of care?

   B. If so, what was the applicable standard of care?

   C. Did the Defendant breach the applicable standard of care?

   D. Did the Defendant’s breach of duty cause damage to the Class?

   Breach of Confidence

   A. Is the Defendant liable for the tort of breach of confidence vis-à-vis Class Members?

Intrusion Upon Seclusion

A. Is the Defendant liable for the tort of intrusion upon seclusion vis-à-vis Class Members?

Damages

A. Can the Court make an aggregate assessment of all or part of the damages suffered by Class Members and, if so, in what amount?

9. The form and content of the notice to the Class and the time and manner for Class Members to opt out of the class proceeding will be determined by further order of the Court.

10. No costs are payable on this certification motion.

"Richard F. Southcott"
Judge

FEDERAL COURT

SOLICITORS OF RECORD

DOCKET:	T-982-20
STYLE OF CAUSE:	TODD SWEET v HER MAJESTY THE QUEEN
PLACE OF HEARING:	VANCOUVER, BRITISH COLUMBIA
DATE OF HEARING:	MAY 11-13, 2022
ORDER AND REASONS:	SOUTHCOTT J.
DATED:	AUGUST 25, 2022

APPEARANCES:

Anthony Leoni Matthew Burtini	FOR THE PLAINTIFF
Sharon Johnston Stephen Kurelek Jamie Hansen	FOR THE DEFENDANT

SOLICITORS OF RECORD:

Rice Harbut Elliott LLP Vancouver, British Columbia	FOR THE PLAINTIFF
Attorney General of Canada Vancouver, British Columbia	FOR THE DEFENDANT