Translated from the original French

SUPERIOR COURT

CANADA
PROVINCE OF QUEBEC
DISTRICT OF MONTREAL

No.: 500-06-001010-194

DATE: August 10, 2023

PRESIDING: THE HONOURABLE BERNARD TREMBLAY, J.S.C.

MICHAEL ROYER
ALA'A ABOU-KHADRA

Plaintiffs

v.

CAPITAL ONE BANK (CANADA BRANCH)
CAPITAL ONE FINANCIAL CORPORATION
CAPITAL ONE BANK (USA) NATIONAL ASSOCIATION
AMAZON.COM.CA INC.
AMAZON.COM INC.
AMAZON WEB SERVICES CANADA INC.
AMAZON WEB SERVICES INC.
AMAZON TECHNOLOGIES INC.

Defendants

CORRECTED JUDGMENT
(on an Application for authorization to institute a class action)

TABLE OF CONTENTS

1. BACKGROUND

[1] The Application for authorization to institute a class action [the Application] invokes the occurrence, on March 22 and 23, 2019, of a confidentiality incident that affects and concerns all individuals who agree on a daily basis to provide their personal information to a considerable number of organizations and entities participants in human activity.

[2] The application was filed by Michael Royer [Royer] on July 30, 2019.

[3] It is directed against Capital One Bank (Canada Branch), Capital One Financial Corporation, and Capital One Bank (USA) National Association [Capital One or the

Capital One group defendants or Capital One], which form one of the largest financial institutions in North America.

[4] The plaintiff Ala'a Abou-Khadra [Abou-Khadra] was added at the time of a subsequent amendment to the application,[1] as were the defendants Amazon.com Inc., Amazon.com.ca Inc., Amazon Web Services Canada Inc., Amazon Web Services Inc., and Amazon Technologies Inc. [Amazon or the Amazon group defendants], which is a recognized electronic commerce giant that provided Capital One with the cloud space permitting the storage of a massive amount of personal information.

[5] This cybernetic incident, as the plaintiffs call it, consisted of the unauthorized access by a former Amazon employee, Paige A. Thompson, of personal information held by that company, initially collected by Capital One and belonging to approximately 6,000,000 Canadian residents and 100,000,000 U.S. residents.

[6] The unfolding of these proceedings was punctuated by four amendments to the application, which now contains over 250 paragraphs, followed by applications filed by the defendants giving rise to interlocutory judgments for the production of additional evidence seeking to counter or complete certain allegations in the Application, and by motions filed by the plaintiffs for authorization to hold written pre-trial examinations.

[7] The plaintiffs also filed a large number of documents describing in great detail the historical and technological background to this intrusion into Amazon's system.

[8] These documents originate especially from other court files in which similar class actions were instituted and which remain active in Canada, but which have since been settled in the United States.[2]

[9] In particular, these documents include the full transcript of the criminal investigation held following the charges laid in the United States by the FBI against Paige A. Thompson, as well as certain evidence filed in the context of this investigation.

[10] A motion to certify a class action filed in Ontario by Rina Del Giudice and Daniel Wood, based on the same events as this case, brought against the Capital One group defendants and the Amazon group defendants, like in this case, was dismissed on August 4, 2021, by the Honourable Paul M. Perell J. of the Ontario Superior Court of Justice.[3]

[11] Procedural issues and other matters of that nature seem to have been determinative in that case.

[12] Another application to certify a class action against only the Capital One group defendants was filed in British Columbia by Duncan Campbell.

---

1 January 29, 2020.
2 Application at para. 10.74 *et seq*.
3 *Del Giudice v. Thompson*, 2021 ONSC 5379.

[13] That application is based on the same events as those invoked in this case, and the class action was certified on June 3, 2022, by the Honourable Nitya Iyer J. of the Supreme Court of British Columbia.[4]

[14] While a reading of these two judgments may be quite instructive and inspiring for the undersigned, and although they were rendered in Canada, these judgments cannot be invoked in this case as having acquired the authority of *res judicata* because they were rendered in other jurisdictions and involve different complainants.

[15] Moreover, those judgments do not bind the Court on the applicable law in this case, even though the complainants have a cause of action that is similar to that of the plaintiffs in this case, because the certification judgments were rendered on the basis of different legal principles, in terms of both class action certification and civil liability, and because those principles come from distinct statutory provisions and common law, and are not applicable in Quebec.

2. ANALYSIS

I. Issues

[16] The plaintiffs claim that the Capital One group defendants and the Amazon group defendants must compensate them solidarily for the injury they suffered, as well as all the putative members of the class identified by the plaintiffs and designated as follows:

> all persons, entities, or organizations resident in Quebec who were either Capital One Credit Card holders or who had applied for a Capital One Credit Card and whose personal and private information was compromised by the incident that occurred on or about March 22 and 23, 2019 (though such breach was only disclosed to the public on July 29, 2019), or any other group to be determined by the Court;

[17] In the conclusions of their Application, the plaintiffs identify twelve (12) questions of fact and of law that they consider to be common to the putative class members and that should be debated before the Court so that it may determine, in the context of the proposed class action, whether the defendants are liable for the damages they claim.

[18] Essentially, they allege that the defendants were negligent for breaching their duty to properly protect the personal information they collected from them and the putative class members over a period of several years, for having kept that information for too long, including the information of members whose credit applications had been refused, and for failing to ensure that the information was hosted in a secure information environment that was adequately protected against intrusions.

---

4 *Campbell v. Capital One Financial Corporation,* 2022 BCSC 928.

[19] More specifically, the applicants, who have all held Costco credit cards issued by Capital One for several years, blame the Capital One group defendants for having migrated around 2015 the personal information belonging to their many clients and that was stored on their servers to a less secure, public hosting site operated by the Amazon group defendants, thereby allowing Paige A. Thompson to access a colossal amount of personal information belonging to them.

[20] The plaintiffs also fault the defendants for failing to have taken the means and measures to prevent this unauthorized access, for being slow to discover it and inform the members, and for failing to subsequently correct the problem that led to the intrusion of this large amount of personal information.

[21] In addition, the plaintiff Abou-Khadra alleges that two transactions that he did not personally make or authorize were charged to his credit card.

[22] As the parties did not insist on this point or present specific evidence in this respect, the Court does not intend to make a distinction in the analysis that follows on the specific liability of any one of the Capital One group defendants as opposed to the other defendants in that group. Similarly, the Court does not intend to distinguish between the specific liability of any one of the Amazon group defendants as opposed to the other defendants in that group.

[23] The Court intends to address the distinctions that may exist between the action the plaintiffs propose to bring against the Capital One group defendants and the action they want to bring against the Amazon group defendants even though there is no contractual relationship between the Amazon group defendants and the plaintiffs or the putative class members in this case.

[24] It should be noted that in their Application, the plaintiffs include an injunctive conclusion against the defendants to require them to implement adequate protection and security measures to prevent and detect any unauthorized access to the personal information they hold.

[25] The wording of this conclusion is extremely broad and imprecise. It is therefore not capable of being subject to specific performance or forced execution, and even less so to a possible conviction for contempt of court, such that this conclusion alone cannot ensure the viability of the proposed class action, or even that it will be allowed at the authorization stage, in the event the Court finds that the plaintiffs have not met the second criterion of article 575 CCP with respect to the damages claimed.

[26] The damages claimed by plaintiffs fall under eleven (11) separate categories that are described in paragraph 6 of the Application.

[27] There are three types: pecuniary, non-pecuniary, and punitive.

[28] First, the plaintiffs claim unquantified pecuniary damages that are essentially to be established or anticipated, for themselves and for all the putative class members, including for the loss of the patrimonial value of their personal information arising from this violation of their private nature, as well as the excessively high membership fees for the services offered by Capital One and obtained from it, which no longer comply with their representations concerning information security.

[29] In this regard, they also claim the expenses they will have to incur to ensure regular verification and monitoring of their accounts and statements over a longer period of time than the two (2) years during which such services were offered to them at no charge by Capital One, as well as the expenses they will have to incur to deal with potential fraud resulting from the theft of their identity, including the expenses required to identify the author of such fraud and put them behind bars, the expenses incurred to cancel the services provided by Capital One and replace them with another financial institution, and the expenses incurred to recover the amounts diverted, and finally, an amount equal to the loss of their rating for the purposes of obtaining credit in the financial markets as a result of this intrusion.

[30] Second, the plaintiffs claim moral and non-pecuniary damages for stress and other trouble and inconvenience of this nature that they have suffered and will continue to suffer as a result of this unauthorized access of their personal information and essentially arising from their fear and anxiety caused by the omnipresent thought of having to live for a long time under the threat of being the potential victims of fraud.

[31] Last, the plaintiffs claim punitive damages from the defendants under section 49 of the *Charter of human rights and freedoms* [the *Charter*][5] resulting from this interference with their right to the protection of their privacy guaranteed by section 5 of the *Charter*, as well as under the mandatory provisions of the *Consumer Protection Act*[6] [the *CPA*], which the defendants violated, in particular through their advertising initiatives and the false or misleading representations they made to the class members regarding the quality of the protection and security of their personal information, the violation of which permits an award of punitive damages under section 272 *CPA* if it is established that it is a prohibited practice.

[32] The first and third criteria set out in article 575 CCP are met in this case, that is, the existence of common issues to be debated and that because of the composition of the proposed Class, there are no means in the CCP other that the class action to assert this common claim of the plaintiffs and the class members.

---

5 CQLR, c. C-12.
6 CQLR, c. P-40.1.

II. The criterion set out in article 575(2) CCP: do the plaintiffs each have an arguable case against the defendants?

(a) The applicable law in this case

[33] Article 575 CCP states:

> The court authorizes the class action and appoints the class member it designates as representative plaintiff if it is of the opinion that
>
> (1) the claims of the members of the class raise identical, similar or related issues of law or fact;
>
> (2) the facts alleged appear to justify the conclusions sought;
>
> (3) the composition of the class makes it difficult or impracticable to apply the rules for mandates to take part in judicial proceedings on behalf of others or for consolidation of proceedings; and
>
> (4) the class member appointed as representative plaintiff is in a position to properly represent the class members.

[34] At the application for authorization stage, the plaintiffs have the burden of demonstrating the value of the legal syllogism they propose in support of an arguable case for each of them to assert against the defendants,[7] not of establishing on a balance of probabilities that they have a sufficient cause of action against each of them.

[35] Indeed, in *Desjardins Financial Services Firm Inc. v. Asselin*,[8] the Supreme Court teaches us that:

> [81] In conclusion, the allegations not only exist and are sufficiently precise, but they are also supported by the evidence in the record. It should be noted that in Quebec, unlike in the rest of the country, an applicant is not required to "show that the claim has a 'sufficient basis in fact'" (*Oratoire*, at para. 58, citing *Infineon*, at para. 128). In this case, requiring conclusive documentary evidence of a failure to provide information would not only ask too much at the authorization stage, but would also impose on Mr. Asselin a burden more onerous than the one he will have to face during the trial on the merits, since an omission can be proved by any means, including testimony and inference.

[36] At the authorization stage, characterized in the case law as one of mere screening,[9] the Court is asked only to determine whether the four criteria set out in article 575 CCP are met.

---

7 *Saurette c. Astrazeneca Canada inc.*, 2019 QCCS 3323.
8 2020 SCC 30.
9 *L'Oratoire Saint-Joseph du Mont-Royal v. J.J.*, 2019 SCC 35.

[37] According to the defendants, the plaintiffs do not meet the requirements arising from the second and fourth criteria set out in article 575 CCP in this case, essentially on the following grounds:

(A) The evidence adduced at the authorization stage reveals that even if Paige A. Thompson successfully accessed the class members' personal information collected by Capital One and hosted in a public cloud space made available to them and managed by Amazon, she did not, as was established during her criminal trial in the United States, communicate this information to a third person or use it in any way, such that neither the plaintiffs, nor the putative class members suffered identity theft and likely never will in connection with this incident;

(B) The defendants did not make any false or misleading representations or commit acts resulting in a contractual or extracontractual fault in regard to the plaintiffs and the putative class members;

(C) In addition, Amazon submits that there is no legal relationship between it and the plaintiffs and the putative class members, because they are identified in the description of the proposed Class as suppliers of Capital One;

(D) Even assuming that the facts alleged by the plaintiffs are true, they do not allege or establish, even by *prima facie* evidence, any compensable injury in support of their application for pecuniary and non-pecuniary damages, instead describing facts and circumstances that do not concern them because they are alleged in other proceedings pending before other jurisdictions in Canada and the United States, such that the damages they claim are purely hypothetical;

(E) With respect to the plaintiff Royer in particular, although he was informed that he was part of the 6,000,000 Canadian residents whose personal information was made accessible during this confidentiality incident on March 22 and 23, 2019, he does not allege or establish any unlawful use of his information or that he suffered any compensable injury, all of which are mere hypotheses, conjecture, or pure speculation;

(F) The plaintiff Abou-Khadra is not part of the group of 6,000,000 Canadian residents who were informed of this intrusion, such that his personal information was simply not made accessible during this incident, whereas the fraud he alleges to have been a target of consists instead of the unauthorized use of his credit card and his security code (CCV), and whereas this information was not made accessible during the incident on March 22 and 23, 2019, and that in his case, this theft is instead the result

of a third person having knowledge of his credit card number and secret code, which is a situation that is foreign to the debate raised in this case;

(G) The pecuniary and non-pecuniary damages claimed by the plaintiffs cannot be awarded under the applicable law in Quebec; these damages are nothing more that the ordinary inconveniences experienced in such circumstances; they are not grave, serious, continuous, or prolonged;[10]

(H) The statutory provisions invoked by the plaintiffs in support of their claim for punitive damages are not applicable in this case; and

(I) Accordingly, neither of the two plaintiffs has an arguable case to assert against the defendants.

[38] The defendants conclude that, due to their particular situations arising from the facts described above, neither of the two plaintiffs can be appointed as the representative plaintiff of the putative class members in order to properly represent them.

[39] In this respect, the plaintiffs note that the facts they allege must be taken as true, unless they are improbable or implausible,[11] and emphasize that the same is not true for the facts alleged by the defendants,[12] as Capital One did in the affidavit of one of its officers, Jeffrey Behan,[13] which it filed further to permission granted under article 574 CCP to present additional evidence.[14]

[40] Thus, the defendants do not have the benefit of this presumption with respect to the probative value of the evidence they adduce.

[41] The plaintiffs add that even if the defendants may have a serious defence to assert on the merits of the case, at this stage the Court must authorize the institution of the proposed class action so long as the Application for authorization proposes an action that may have merit,[15] and so long as it does not seem frivolous or clearly unfounded on its face.[16]

[42] According to the defendants, the difficulty in this case lies not in the Court's determination of the facts it must accept among those alleged by the plaintiffs or the defendants because the parties put forward contradictory versions, which is not the case

---

[10] *Mustapha v. Culligan,* 2008 SCC 27; *Zuckerman v*. *MGM Resorts International*, 2022 QCCS 2914.
[11] *Option Consommateurs c*. *Google*, 2022 QCCS 2308.
[12] *Durand c*. *Subway Franchise Systems of Canada*, 2020 QCCA 1647.
[13] September 29, 2021.
[14] *Benamor c. Air Canada*, 2020 QCCA 1597.
[15] *M.L. c*. *Guillot*, 2021 QCCA 1450.
[16] *Société québécoise de gestion collective des droits de reproduction (Copibec) c*. *Université Laval*, 2017 QCCA 199.

here. Nor is it that the factual background presented by the plaintiffs is contested, because it is not really questioned by the defendants in this case.

[43] Instead, the difficulty here resides in the fact that, according to the defendants, the allegations of injury suffered set out in the Application are hypothetical, speculative, and purely theoretical, because the Application fails to set out a genuine, arguable cause of action against them and this confidentiality incident ultimately had no impact on the plaintiffs or on the putative class members.

[44] The defendants therefore invite the Court to note the absence of specific facts alleged by the plaintiffs regarding the impact of this access on their personal information and, accordingly, to find that there is no arguable cause of action to assert against them, as there is no compensable injury.

[45] The defendants also argue that the facts alleged by the plaintiffs, combined with those revealed by the additional evidence they were authorized to present, clearly and unequivocally show that there is no legal syllogism supporting an arguable cause of action in favour of the plaintiff Abou-Khadra because his personal information was not the subject of this intrusion, as the unauthorized purchases made on his credit card have no connection with this cybernetic event that took place in March 2019.

[46] At this stage of the analysis, it is appropriate to recall that each plaintiff must establish the existence of an arguable cause of action specific to him against the defendants, independent of the fact that the class members may have such a cause of action themselves.[17]

[47] With respect to the plaintiff Royer, the defendants add that he suffered no particular injury even though he was informed on August 14, 2019, of this confidentiality breach that occurred on March 22 and 23, 2019, in the information security system implemented by the defendants, because his personal information was not reproduced, distributed, or used, according to what is stated in Paige A. Thompson's deposition.

[48] Therefore, this plaintiff has not had to make or incur any disbursements and will not have to cover any expenses whatsoever, other than having to live with the ordinary inconveniences in similar circumstances,[18] it being understood that Capital One offered to cover the costs of verifying and monitoring his and the putative class members' credit card accounts and statements.

[49] Last, Amazon adds that it has no legal relationship with the plaintiffs or with the putative class members, because it dealt only with Capital One in this matter, as indicated in the allegations in the Application and the supporting exhibits invoked, including the

---

[17] *Sofio c. Organisme canadien de réglementation du commerce des valeurs mobilières (OCRCVM)*, 2015 QCCA 1820.

[18] *Supra* note 10.

application forms issued by Capital One, the standard form contract it currently uses, and its confidentiality policy stated therein.

[50] However, in an excerpt from the website of the defendant Amazon Web services Canada Inc.,[19] it presents English and French versions of the services it offers to consumers in Canada for the preservation of their personal information.

[51] The plaintiffs submit that if Capital One cannot be found at fault under the regime of contractual liability, each of the defendants have nevertheless incurred their extracontractual liability towards them and the putative class members under article 1457 CCQ, which states:

> 1457. Every person has a duty to abide by the rules of conduct incumbent on him, according to the circumstances, usage or law, so as not to cause injury to another.
>
> Where he is endowed with reason and fails in this duty, he is liable for any injury he causes to another by such fault and is bound to make reparation for the injury, whether it be bodily, moral or material in nature.
>
> He is also bound, in certain cases, to make reparation for injury caused to another by the act, omission or fault of another person or by the act of things in his custody.

[52] The plaintiffs allege that in addition to their right to the protection of their privacy guaranteed by section 5 of the *Charter*, the defendants also violated articles 35 to 37 CCQ and the relevant provisions of the *Personal Information Protection and Electronic Documents Act*[20] [*PIPEDA* or the *Federal Act*] and of the *Act respecting the protection of personal information in the private sector*[21] [the *Quebec Act*].

[53] Indeed, section 5 of the *Charter* states that every person has a right to respect for his private life, and this section applies to the defendants in Quebec.

[54] The Quebec *Act respecting the protection of personal information in the private sector* defines the scope of its application as follows:

> **1.** The object of this Act is to establish, for the exercise of the rights conferred by articles 35 to 40 of the Civil Code concerning the protection of personal information, particular rules with respect to personal information relating to other persons which a person collects, holds, uses or communicates to third persons in the course of carrying on an enterprise within the meaning of article 1525 of the Civil Code.

---

19 Exhibit R-6.
20 S.C. 2000, c. 5.
21 CQLR, c. P-39.1.

> The Act applies to such information whatever the nature of its medium and whatever the form in which it is accessible, whether written, graphic, taped, filmed, computerized, or other.
>
> This Act also applies to personal information held by a professional order to the extent provided for by the Professional Code (chapter C-26).
>
> This Act does not apply to journalistic, historical or genealogical material collected, held, used or communicated for the legitimate information of the public.
>
> Divisions II and III of this Act do not apply to personal information which by law is public.
>
> **2.** Personal information is any information which relates to a natural person and allows that person to be identified.
>
> **3.** This Act does not apply
>
> (1) to a public body within the meaning of the Act respecting Access to documents held by public bodies and the Protection of personal information (chapter A-2.1);
>
> (2) to information held on behalf of a public body by a person other than a public body.
>
> **3.1.** Any person carrying on an enterprise is responsible for protecting the personal information held by the person.
>
> Within the enterprise, the person exercising the highest authority shall see to ensuring that this Act is implemented and complied with. That person shall exercise the function of person in charge of the protection of personal information; he may delegate all or part of that function in writing to any person.
>
> The title and contact information of the person in charge of the protection of personal information must be published on the enterprise's website or, if the enterprise does not have a website, be made available by any other appropriate means.
>
> [Emphasis added.]

[55] This Quebec statute thus applies to any person carrying on an enterprise in Quebec who holds personal information on a natural person allowing the person to be identified.

[56] Sections 3.5, 10, 28, and 29 of the *Quebec Act* also set out specific obligations regarding the protection, security, prevention, and diligence incumbent on enterprises subject to the *Act* when a confidentiality incident occurs:

> **3.5** Any person carrying on an enterprise who has cause to believe that a confidentiality incident involving personal information the person holds has occurred must take reasonable measures to reduce the risk of injury and to prevent new incidents of the same nature.
>
> If the incident presents a risk of serious injury, the person carrying on an enterprise must promptly notify the Commission d'accès à l'information established by section 103 of the Act respecting Access to documents held by public bodies and the Protection of personal information (chapter A-2.1). He must also notify any person whose personal information is concerned by the incident, failing which the Commission may order him to do so. He may also notify any person or body that could reduce the risk, by communicating to the person or body only the personal information necessary for that purpose without the consent of the person concerned. In the latter case, the person in charge of the protection of personal information must record the communication of the information.
>
> **10.** A person carrying on an enterprise must take the security measures necessary to ensure the protection of the personal information collected, used, communicated, kept or destroyed and that are reasonable given the sensitivity of the information, the purposes for which it is to be used, the quantity and distribution of the information and the medium on which it is stored.
>
> **28.** In addition to the rights provided under the first paragraph of article 40 of the Civil Code, the person concerned is entitled to obtain that any personal information collected otherwise than according to law be deleted.
>
> **29.** Every person carrying on an enterprise who holds files on other persons must take the necessary steps to ensure the exercise by a person concerned of the rights provided under articles 37 to 40 of the Civil Code and the rights conferred by this Act. In particular, he must inform the public of the place where, and manner in which, access to the files may be granted.
>
> [Emphasis added.]

[57] As the provisions cited above reveal, this legislation implements the exercise of the rights conferred by articles 35 to 40 CCQ with respect to the protection of personal information by setting out specific rules regarding the personal information relating to other persons that a person collects, holds, uses, or communicates to third persons in the course of carrying on an enterprise within the meaning of article 1525 CCQ.

[58] It seems quite obvious that these statutory provisions provide a legal framework of standards that enterprises such as the one operated by the defendants in Quebec must comply with.

[59] Moreover, articles 35 to 37 CCQ state:

> **35.** Every person has a right to the respect of his reputation and privacy.
>
> The privacy of a person may not be invaded without the consent of the person or without the invasion being authorized by law.
>
> **36.** The following acts, in particular, may be considered as invasions of the privacy of a person:
>
> (1) entering or taking anything in his dwelling;
>
> (2) intentionally intercepting or using his private communications;
>
> (3) appropriating or using his image or voice while he is in private premises;
>
> (4) keeping his private life under observation by any means;
>
> (5) using his name, image, likeness or voice for a purpose other than the legitimate information of the public;
>
> (6) using his correspondence, manuscripts or other personal documents.
>
> **37.** Every person who establishes a file on another person shall have a serious and legitimate reason for doing so. He may gather only information which is relevant to the stated objective of the file, and may not, without the consent of the person concerned or authorization by law, communicate such information to third persons or use it for purposes that are inconsistent with the purposes for which the file was established. In addition, he may not, when establishing or using the file, otherwise invade the privacy or injure the reputation of the person concerned.

[60] As we will see below, article 1525 CCQ addresses the presumed solidarity between debtors where an obligation is contracted for the service or operation of an enterprise.

[61] The *Federal Act*, for its part, concerns the personal information and electronic documents handled by an enterprise subject to that *Act*.

[62] In this case, as set out in its section 30, it could apply to the extent that the National Assembly of Quebec does not have the power to enact a statute on the collection, use, or disclosure of personal information or if a person discloses the information outside the province for consideration, which could be the case for the defendants, but the evidence is not sufficiently eloquent on this point:

> **30.** This Part does not apply to any organization in respect of personal information that it collects, uses or discloses within a province whose legislature has the power

> to regulate the collection, use or disclosure of the information, unless the organization does it in connection with the operation of a federal work, undertaking or business or the organization discloses the information outside the province for consideration.
>
> [Emphasis added.]

[63] The National Assembly has the power to regulate this activity and in fact exercised that power when it enacted the *Quebec Act* cited above.

[64] The *Federal Act* may also apply to Capital One and to Amazon if they are considered to be federal works, undertakings, or businesses, or if in this case they have disclosed the personal information they hold in another Canadian province for consideration.

[65] The evidence adduced at this stage does not allow the Court to rule definitively on this issue, which must be the subject of debate before the judge hearing this case on the merits.

[66] The *Federal Act* specifically provides for the possibility of filing a complaint with the Privacy Commissioner of Canada and states that the Federal Court of Canada has jurisdiction in such matters to hear any issue in respect of which a complaint was made or to grant a remedy, including an award of damages.[22]

[67] The provisions of the *Charter*, the *Quebec Act* on personal information, and the *Civil Code of Québec* cited above are therefore certainly applicable to the defendants in this case, at least at first glance, with respect to the statutory obligations that may be incumbent on them in matters of personal information; the provisions of the *Federal Act* may also apply, but this will have to be established at the hearing on the merits of this case.

[68] As mentioned above, the plaintiffs also claim punitive damages under section 49 of the *Charter of human rights and freedoms* and section 272 *CPA*.

[69] With respect to the application of section 272 *CPA* to this case, the plaintiffs rely on sections 34, 40 to 42, 215 to 219, 228, 253, and 271 of the *CPA* to assert that the defendants engaged in a prohibited practice under that *Act*. These provisions state:

> **34.** This division applies to contracts of sale or lease of goods and to contracts of service.
>
> **…**

[22] Sections 11 to 16 *PIPEDA*.

40. The goods or services provided must conform to the description made of them in the contract.

41. The goods or services provided must conform to the statements or advertisements regarding them made by the merchant or the manufacturer. The statements or advertisements are binding on that merchant or that manufacturer.

42. A written or verbal statement by the representative of a merchant or of a manufacturer respecting goods or services is binding on that merchant or manufacturer.

43. A warranty respecting goods or services that is mentioned in a statement or advertisement of the merchant or the manufacturer is binding on that merchant or that manufacturer. This rule applies to the written warranties of the merchant or the manufacturer not written in the contract.

…

215. Any practice contemplated in sections 219 to 251.2 or, in case of the sale, lease or construction of an immovable, in sections 219 to 222, 224 to 230, 232, 235, 236 and 238 to 243 constitutes a prohibited practice for the purposes of this title.

216. For the purposes of this title, representation includes an affirmation, a behaviour or an omission.

217. The fact that a prohibited practice has been used is not subordinate to whether or not a contract has been made.

218. To determine whether or not a representation constitutes a prohibited practice, the general impression it gives, and, as the case may be, the literal meaning of the terms used therein must be taken into account.

219. No merchant, manufacturer or advertiser may, by any means whatever, make false or misleading representations to a consumer.

…

228. No merchant, manufacturer or advertiser may fail to mention an important fact in any representation made to a consumer.

…

253. Where a merchant, manufacturer or advertiser makes use of a prohibited practice in case of the sale, lease or construction of an immovable or, in any other case, of a prohibited practice referred to in paragraph a or b of section 220, a, b, c, d, e or g of section 221, d, e or f of section 222, c of section 224 or a or b of section 225, or in section 227, 228, 229, 237 or 239, <u>it is presumed that had the consumer been aware of such practice, he would not have agreed to the contract or would not have paid such a high price</u>.

…

> **271.** If any rule provided in sections 25 to 28 governing the making of contracts is not observed or if a contract does not conform to the requirements of this Act or the regulations, the consumer may demand the nullity of the contract.
>
> In the case of a contract of credit, if any of the terms and conditions of payment, or the computation or any indication of the credit charges or the credit rate does not conform to this Act or the regulations, the consumer may at his option demand the nullity of the contract or demand that the credit charges be cancelled and that any part of them already paid be restored.
>
> The court shall grant the demand of the consumer unless the merchant shows that the consumer suffered no prejudice from the fact that one of the above mentioned rules or requirements was not respected.
>
> **272.** 272. If the merchant or the manufacturer fails to fulfil an obligation imposed on him by this Act, by the regulations or by a voluntary undertaking made under section 314 or whose application has been extended by an order under section 315.1, the consumer may demand, as the case may be, subject to the other recourses provided by this Act,
>
> (a) the specific performance of the obligation;
>
> (b) the authorization to execute it at the merchant's or manufacturer's expense;
>
> (c) that his obligations be reduced;
>
> (d) that the contract be rescinded;
>
> (e) that the contract be set aside; or
>
> (f) that the contract be annulled,
>
> without prejudice to his claim in damages, in all cases. He may also claim punitive damages.
>
> [Emphasis added.]

[70] As for the application of section 272 *CPA*, the plaintiffs must first meet the four requirements set out by the Supreme Court in *Richard v. Time Inc*.,[23] which provides an analytical framework to determine the application of the presumption of prejudice set out in the *CPA* in the event of a prohibited practice:

> [124] This absolute presumption of prejudice presupposes a rational connection between the prohibited practice and the contractual relationship governed by the Act. It is therefore important to define the requirements that must be met for the presumption to apply in cases in which a prohibited practice has been used. In our opinion, a consumer who wishes to benefit from the

[23] 2012 SCC 8.

> presumption must prove the following: (1) that the merchant or manufacturer failed to fulfil one of the obligations imposed by Title II of the Act; (2) that the consumer saw the representation that constituted a prohibited practice; (3) that the consumer's seeing that representation resulted in the formation, amendment or performance of a consumer contract; and (4) that a sufficient nexus existed between the content of the representation and the goods or services covered by the contract. This last requirement means that the prohibited practice must be one that was capable of influencing a consumer's behaviour with respect to the formation, amendment or performance of the contract. Where these four requirements are met, the court can conclude that the prohibited practice is deemed to have had a fraudulent effect on the consumer. In such a case, the contract so formed, amended or performed constitutes, in itself, a prejudice suffered by the consumer. This presumption thus enables the consumer to demand, in the manner described above, one of the contractual remedies provided for in s. 272 *C.P.A.*
>
> [Emphasis added.]

[71] However, once a person's negligent and reckless attitude towards others, the public, or a consumer is established, such conduct can essentially be assimilated to an intentional interference or violation;[24] the same is true when that person acts with full knowledge of the immediate and natural or at least extremely probable consequences that his or her conduct will cause.[25]

[72] According to the plaintiffs, the defendants acted with such negligence towards the plaintiffs and the putative class members in this case, because they made representations on the reliability of their information security system with full knowledge of the vulnerability of that hosting system used to keep the members' personal information since at least 2015.

[73] The plaintiffs add that the defendants, through their public representations and their advertising in general, on both their application form and their respective websites, in particular with respect to Capital One and its confidentiality policy discussed below, and Amazon, perhaps to a different extent, made false or misleading representations to the plaintiffs and to the class members, which constitute prohibited practices under section 215 et *seq*. of the *CPA*, cited above.

[74] The plaintiffs conclude that pursuant to sections 253 and 271 of the *CPA*, the class members benefit from both this presumption of the existence of a prohibited practice that led to their membership with Capital One and the presumption that the class members suffered prejudice without it being necessary for them to prove it, such that the

---

[24] Dallaire, Claude, "L'évolution des dommages exemplaires depuis les décisions de la Cour suprême en 1996 - dix ans de cheminement" in *Développements récents en droit administratif et constitutionnel* (Barreau du Québec – Service de la formation continue, 2006) at 249–252.

[25] *Levy c. Nissan Canada inc*., 2021 QCCA 682.

defendants must pay punitive damages under section 272 *CPA*, and the plaintiffs need only prove the existence of false or misleading representations, without having to establish prejudice.

[75] According to the defendants, these provisions are not applicable to the credit contract that may bind the plaintiffs and the class members to the Capital One group defendants, because sections 40 to 42 of the *CPA* are found in a specific section of the statute dealing solely with contracts of sale or lease of goods and to contracts of service, not credit contracts.

[76] They refer in particular to section 36 *et seq*. of the *CPA*, in Chapter III, concerning contracts of sale or lease of goods and contracts of service.

[77] First, the Court notes that Title 1 of the *CPA* applies to all contracts concerning a good or a service, and that Chapter I sets outs the provisions that are generally applicable to all these contracts.

[78] In Chapter III, still under Title 1, the *CPA* deals generally with contracts involving the sale or lease of goods or services and provides, in Division I, general obligations applicable to these contracts that are necessarily in addition to those set out in Chapter I discussed above.

[79] Next, Chapter III focusses on specific, and again additional, obligations in different divisions, including Division III on contracts of credit, to be applied to various types of consumer contracts, according to the nature of the specific contract referred to in each of these divisions, including credit contracts, which nevertheless remain subject to the general obligations applicable to contracts of sale or lease of goods or services set out in Chapter I.

[80] In this case, the consumer contract binding the putative class members and Capital One is, according to the terms of the *CPA*, governed not only by the specific provisions regarding contracts of credit set out in that *Act*, because the consumer contract invoked here is a contract for services concerning various financial services, including credit, but also by the general provisions set out in Chapter I, Title I of the *CPA*, including section 40 *et seq*. of that *Act*.

[81] In addition, nothing in the authorities cited by the defendants indicates that the general provisions set out in section 35 *et seq*. of the *CPA* concerning contracts of sale, lease of goods, and of service do not apply to the specific contract of service relating to the issuance by Capital One of a credit card to the members.

[82] Accordingly, the consumer contract entered into between the plaintiffs and the putative class members on the one hand, and Capital One on the other, may be governed by the provisions of the *CPA*.

(b) The plaintiff Abou-Khadra

[83] The plaintiff Abou-Khadra makes no allegation and adduces no evidence permitting the Court to establish, even *prima facie*, that his personal information was the target of unauthorized access during this confidentiality incident that occurred in March 2019. Moreover, it is established that he is not part of the 6,000,000 Canadian residents that were informed by the Capital One group defendants of this event, to which another 51,000 Canadian residents were added.

[84] The facts he alleges and those related by Capital One in the context of the additional evidence it was authorized to present by means of the affidavit of Jeffrey Behan on September 29, 2021, referred to above, clearly and unambiguously reveal that these two unauthorized transactions on this plaintiff's credit card statement, for amounts of $267 and $2.55,[26] are unrelated to the confidentiality incident that occurred on March 22 and 23, 2019.

[85] According to Mr. Behan's affidavit, the two transactions on the plaintiff Abou-Khadra's credit card statement[27] are the result of the use of his credit card number, given by telephone to the merchant in question, in this case Power Keto, as well as his secret code found on the back of his credit card, which was also disclosed by telephone to this merchant.

[86] Also according to Mr. Behan's affidavit, however, no bank account, credit card, secret code, or social insurance number was the subject of this confidentiality breach on March 22 and 23, 2019.

[87] Last, it should also be noted that the facts alleged in Mr. Behan's affidavit provided by Capital One are uncontradicted.

[88] On the basis of this evidence, the Court cannot, as the plaintiffs propose, apply this notion of contemporaneity or timing between the events that occurred on March 22 and 23, 2019, and the unauthorized transactions added to Abou-Khadra's account, because specific evidence was presented in this case to set aside this possibility or hypothesis in the form of a kind of presumption arising simply from the temporal proximity of these two events.

[89] In addition, in the conclusions of the proposed class action with respect to the Class and in the notices to be given to the class members, the plaintiffs themselves exclude the persons in the same situation as the plaintiff Abou-Khadra, because these persons cannot be properly identified and because the designated Class of members identifies those whose data was compromised during the March 2019 incident, which excludes the plaintiff Abou-Khadra.

---

[26] Exhibit P-29.
[27] Exhibit R-29.

[90] Therefore, the proposed class action will not be authorized with respect to this plaintiff.

(c) Capital One

Fault

[91] In support of the legal syllogism they invoke against Capital One, the plaintiffs rely on the application form it published in 2019, which they each used several years earlier at the time of their respective enrollment for one of the six categories of credit cards offered[28] by this financial institution.

[92] This form requires various personal information from the persons who fill out the application for membership,[29] including their social insurance number, to obtain a Costco credit card issued by Capital One.

[93] The plaintiffs then refer to the documents published on Capital One's website,[30] in which the terms and conditions of the 2020 version of its confidentiality policy are set out, and to texts describing the security measures implemented by Capital One.

[94] The plaintiffs rely on these documents not only to establish Capital One's contractual fault against the putative class members, but also to support the existence of its false or misleading representations, as of 2015 in particular, on the protection and security measures it implemented to protect the private and confidential nature of their personal information.

[95] An excerpt of Capital One's confidentiality policy follows:[31]

> Keeping your information safe and secure is very important to us. We want you to know what we're doing to protect your information, and what you can do to help.
>
> It's unlikely that unauthorized transaction would happen through online banking or that information obtained from the online banking site would result in the unauthorized use of your credit card account. However, il it ever does occur, don't worry – as a Capital One cardholder, you're protected
>
> **How we keep your information safe**
>
> Our strong encryption technology ensures that any data that passes between your computer and our server is secure.

28 Exhibit R-7.
29 Exhibit R-8.
30 Exhibits R-11 and R-15.
31 Exhibit R-15.

- We use firewalls systems and intrusion detection software to prohibit unauthorized access to our systems

- Our VeriSign Secure Socket Layer Certificate (https://sealinfo.verisign.com/splash?form file=fdf/splash.fdf&lang=en&en=servicing.capitalone.com) means you can be extra confident that banking online with us is secure

- We automatically send you an alert informing you of any changes made to you online banking profile

- The online banking website will automatically log off after a period of inactivity during any session to protect your information.

[Emphasis added.]

[96] The preceding excerpts of the confidentiality policy and those set out below reveal that the parties agreed to incorporate into their contract the definition of the term [TRANSLATION] "Confidential information" set out in the *Federal Act* (*PIPEDA*), which, that being said, does not make that law applicable to the parties in this case,[32] as discussed above, such that only this definition is incorporated into the contract binding the parties.

[97] These excerpts state that Capital One undertakes to use this information in particular to prevent fraud and for the purposes set out in the applicable legislation and industry standards.

[98] According to the plaintiffs, the documents referred to above read in much the same way when they signed up. They note that the relevant versions can be obtained in a timely manner before the hearing on the merits of the case.

[99] The other documents consist of notices and communiqués found on the defendants' websites.[33]

[100] In support of their plan of argument dated December 19, 2022, the plaintiffs refer to a more complete document titled Customer Agreement, which sets out the terms and conditions of the consumer contract concluded between the members and Capital One.[34]

[101] They filed this contract, under objection, however,[35] in order to set out the full content of this document, including all the terms and conditions of Capital One's confidentiality policy with respect to the personal information obtained from its clients.

---

32 *Ibid*.

33 Exhibits R-6 and R-58.

34 Exhibit R-93, 2022 version.

35 The defendants submit that documents R-8, R-15, R-16, and R-93 date from after 2015 and add in regard to the last exhibit, and for exhibits R-94 and R-95, that this manner of proceeding by the plaintiffs is irregular and unlawful in that the documents they invoke must be alleged and invoked as exhibits in

[102] The Court reproduces a few excerpts below:[36]

Information we collect

Information we collect about our customers includes, but is not limited to:

- Publicly available information, such as information from telephone or other public directories;
- The information you provided to us before you became a customer;
- Information about your transactions, including purchases, account balances, fees, payment history, parties to transactions and credit card usage;
- Information from credit reporting agencies and other outside sources to verify financial information about you, such as your employment and credit history;
- Information from surveys that customers participate in, or from third parties that customers engage with;
- Information from customers' mobile and online activity (for example, IP address, mobile device ID, application and website use, and history); and
- Information required by law.

Use of Information

Purposes that we use your information for include, but are not limited to:

- Contacting and authenticating you;
- Assessing your creditworthiness;
- Making improvements to products and services;
- Preventing fraud;
- Serving you offers, advertising and marketing;
- Maintaining, servicing, processing, analyzing, auditing and collecting on your account(s); and
- Sharing information with consumer reporting agencies and other parties who have financial, employment or business dealings with you.

Consent

If you apply for a credit product, communicate with us or provide information to us in any way, you acknowledge your consent for personal information collection, use and disclosure as set out in our Policy, applicable laws and/or industry standards. You can withdraw your consent for use and disclosure of your personal information, other than that which is required for us to maintain

support of the Application, not of their plan of argument, which was remedied at the hearing by an oral application to amend the Application.

[36] Exhibit R-93.

> and service your account, subject to legal and contractual restrictions, with reasonable notice to us.
>
> **Limiting collection**
>
> We only collect personal information that's necessary for the purposes we identify, and as required by applicable laws.
>
> **Limiting use, disclosure and retention**
>
> We limit use, disclosure and retention of personal information to the purposes we identify, and as required by applicable laws. We may share your personal information with service providers who perform services on our behalf. Our contracts with third parties include obligations to protect your personal information. Your personal information may be stored and processed at our corporate offices in the U.S. or with approved third parties within the U.S. or elsewhere. If a third party processes or stores information outside of Canada, foreign governments, courts or regulatory agencies may be able to obtain such personal information through the laws of the foreign jurisdiction.
>
> [Emphasis added.]

[103] Certain documents were mentioned for the first time in the plaintiffs' plan of argument filed for the hearing of the Application,[37] despite the four amendments made to it.

[104] The plaintiffs justify their actions by the unavailability of these documents before the hearing and that they finally and undoubtedly obtained them further to a search in the two other similar court cases referred to above that remain pending in Canada.[38]

[105] In this regard, the Court cannot block the plaintiffs' submissions based on the sole fact that they rely on documents dating from a few years after the incident that occurred in 2019 and reprimand them for it, because at this stage, it can simply rely on the plaintiffs' allegations, which they will eventually have to prove, that such undertakings were set out in these documents at the time of the plaintiffs' enrollment several years earlier, presumably in 2005.

[106] This difficulty obtaining all the relevant data and documents is inherent to all applications at the authorization stage, and it can be overcome at the trial stage of this case, as Kasirer J.A. noted in *Asselin*,[39] after pre-trial examinations are held and other pre-trial means of proof are implemented.

---

37 Exhibits P-93 to P-95.

38 See the excerpts reproduced in the two judgments cited above of Perell and Iver JJ., *supra* notes 3 and 4.

39 *Supra* note 9.

[107] The plaintiffs fault Capital One for having kept for many years personal information that had become objectively useless with the passage of time and other information without justification because it was obtained from persons who had been refused the credit sought.

[108] According to the plaintiffs, even though it had become useless, this information, which remains private and confidential to this day, nevertheless continued to further the defendants' commercial objectives and the lucrative projects they promoted.

[109] The conservation period for some of this personal information extended up to 14 years, from the time of the plaintiffs' enrollment to the date of the confidentiality incident, and according to the information obtained by the plaintiffs, it was kept solely for the purpose of the development of artificial intelligence software by Amazon, in particular to probe the credit and consumption habits of the members in order to offer them new products and services.

[110] The plaintiffs explain in their Application and also argued at the hearing, relying on articles written by industry observers published on the web and in specialized journals,[40] that in October 2015, Capital One migrated the personal information it held at the time, which had become inevitable due to the excessively large quantity of data in question, to Amazon's servers, which are public and less airtight, and therefore less secure than those of Capital One.

[111] Of course, a former employee of the defendant Amazon Web Services Inc., was responsible for the unauthorized access on March 22 and 23, 2019, but according to Amazon, this intrusion was caused by the improper configuration by Capital One of a required protection system that had to be installed at the time of this massive migration of personal information held by Capital One,[41] and this deficiency was exacerbated by the excessively broad access granted by Capital One.

[112] The plaintiffs state that the cause of this confidentiality incident is instead the deficient architecture chosen by Capital One, but that its implementation was made possible only through Amazon's assistance, such that it was because of the mutual choice by Capital One and Amazon of this process, called Cloud Custodian, which was supposed to protect their system against all vulnerabilities, that this unfortunate confidentiality was able to occur and that it could not have been foreseen or prevented.[42]

[113] Moreover, the allegations in the Application and certain exhibits[43] describe a form of association between Capital One and Amazon during the implementation of this environment for keeping and hosting personal information and its treatment by various

---

40 Exhibits R-11 to R-13.
41 Exhibits R-39 a) and b).
42 Application at para. 10.58 and exhibit R-14.
43 Exhibits R-12.

software they had developed, essentially by Amazon, to optimize their product and service offering and their sales.

[114] Potential recourses may eventually be considered between Capital One and Amazon, perhaps in this proceeding or in another, but such recourses are of little importance at this stage of the analysis, because it is sufficient for the Application to reveal the possibility that a contractual fault may have been committed by Capital One, to whom the putative class members entrusted their personal information, for the plaintiffs to pass the first step of this screening stage.

[115] This public cloud service managed by Amazon is described as being made up of considerable basins or lakes of data and is considered within the entire industry as being less reliable than other similar systems, such that it is viewed with skepticism and avoided by various financial institutions and even by other large technology companies such as Google and Microsoft, because it represents a higher risk for information security system breaches.

[116] This significant vulnerability was previously in the spotlight for incidents that occurred in the United States between 2016 and 2019 giving rise to sanctions imposed on the Capital One group defendants by the American oversight body having jurisdiction over such matters[44] in connection with the internal risk assessment processes implemented by Capital One,[45] outlined generally in several applications to certify class actions filed in the United States that were eventually joined before a single US jurisdiction.[46]

[117] The plaintiffs also relate that further to the unauthorized access on March 22 and 23, 2019, the vulnerability of Amazon's system to such intrusions [called SSRF] was signalled on April 14, 2019,[47] by one of its employees to his superior,[48] but despite this, Capital One was slow in responding as it discovered the intrusion only on July 17, 2019, following a communication from a third person, while the astronomical volume of compromised information that had been rendered accessible included names, addresses, telephone numbers, dates of birth, social insurance numbers, and other data on the credit records of the millions of persons concerned.

[118] The plaintiffs add that Capital One was also negligent subsequently by failing to diligently inform its clients of this intrusion, and finally for having offered them only a quite imperfect and insufficient solution consisting of two years of free service provided by external firms such as Equifax and TransUnion monitoring the entries recorded in their

---

44 *US Office of the Comptroller of the Currency.*
45 Application at para. 10.74 *et seq*.
46 Which was the subject of a transaction on January 31, 2022, before the presentation of the application for certification scheduled for the next day.
47 Exhibit R-18.
48 Exhibit R-89.

statements of account to detect any irregularity that may result from an unlawful appropriation of private and confidential data.

[119] In this regard, the plaintiffs submit that several class members expressed their dissatisfaction with this offer of free monitoring of their accounts for two years, arguing that they could nevertheless be the victims of fraud and data and identity theft, without it being detected, and considering that the risk of such an unlawful act extends far beyond a period of two years, such that the class members will incur hundreds of dollars in monitoring fees every year.

[120] Finally, the plaintiffs note that the defendants nevertheless subsequently maintained this deficient protection and security system,[49] even though the Canadian Imperial Bank of Commerce has been issuing the Costco banner's credit cards since April 2022.

[121] As a result of the foregoing, the Court is of the view that the allegations in the Application reveal that Capital One may have committed a contractual fault against the plaintiff Royer and the putative class members leading to this unauthorized intrusion into their personal information in March 2019.

[122] Indeed, the documents invoked by the plaintiffs[50] contain statements that are sufficient to support the existence of a contractual fault by Capital One against Royer and the putative class members, including by reference to the applicable legislative and industry standards, particularly with respect to the risks associated with this data migration in 2015, and by the implementation of insufficient and ineffective protection measures despite indications and alerts from different industry actors and the competent regulatory authorities, which were ignored by Capital One.

[123] This potential fault by Capital One may also arise from keeping data concerning some members who had been refused credit, and for a large number of them, over an unreasonably long period.

[124] This fault thus arises from Capital One's potential breach of the undertakings flowing from its application form filled out by the putative class members[51] and from the resulting consumer contract entered into between the parties, incorporating the confidentiality policy concerning the personal information obtained from its clients, which documents also refer to the applicable legislation and regulations, including the provisions set out above of the Quebec *Act respecting the protection of personal information in the private sector*, the CCQ, and perhaps the *Federal Act*.

[125] Therefore, despite the terms of the contract Capital One entered into with the members, the statutory provisions it was subject to, and the information security

---

49 Application at para. 10.59.
50 *Ibid*.
51 Exhibits R-8, R-15, R-58, and R-93.

standards recognized in the industry, Capital One failed to adequately protect the personal information of its clients and their right to the protection of their privacy and to take all required means or exercise the basic necessary prudence and diligence normally required and that the putative class members could expect, thereby violating its contractual obligations, including the statutory obligations set out above and applicable to it, at the time of this unauthorized intrusion in March 2019. Next, it failed to warn of this confidentiality incident that had become possible if not probable following this massive migration of the personal information of its clients in 2015 to the cloud service offered by Amazon, and to subsequently remedy the deficiencies in its system.

False or misleading representations

[126] The plaintiffs also fault Capital One for having falsely represented to its clients for many years the value and reliability of its protection and security system for the personal information obtained from its clients, thereby inciting its clients to entrust their personal information to it.

[127] The plaintiffs rely on the same documents referred to above to establish Capital One's fault against the putative class members, but this time to argue that it made false or misleading representations, in particular in 2015 on the protection and security measures apparently implemented to protect the private and confidential nature of their personal information.[52]

[128] The plaintiffs therefore again invoke the content of these contractual documents regarding Capital One, and the excerpts from its website, to describe these false or misleading representations with respect to Amazon as well, as we will see below.[53]

[129] First of all, the application is silent with respect to whether the plaintiffs could take note of the content of all these documents before filling out their Capital One application forms and contracting with it.

[130] In addition, nothing in the allegations of the Application shows that any information provided to the plaintiffs and the class members by Capital One, or published by it, subsequently turned out to be false or misleading at any time between 2015 and 2019.

[131] The confidentiality incident that occurred in March 2019 can certainly be invoked to establish the existence of a fault, but the fact remains that none of the allegations in the Application specifically identifies a particular representation, written or oral, made in the past by Capital One, that is false or misleading in this respect and that was made with the aim of inciting the class members to contract with it.

[132] Thus, even if a consumer contract was concluded between the plaintiffs and the class members on the one hand, and Capital One on the other, thereby making the *CPA*

---

52 Exhibits R-15 and R-16.
53 Exhibits R-6, R-11, and R-15.

applicable to Capital One, the Court is of the view that the evidence presented to it and the allegations in the Application are insufficient and too vague, general, and imprecise to find that Capital One may have made such false or misleading representations to the class members within the meaning of that expression in the *CPA* to constitute a prohibited practice under the *CPA*, permitting the class members to claim punitive damages from it under section 272 *CPA*.

(d) Amazon

Fault

[133] Amazon argues that it has no legal relationship with the putative class members, but only with Capital One, and that this contractual relationship consists only of allowing Capital One to host on its cloud the personal information obtained from Capital One's clients who live in Quebec.

[134] According to Amazon, it did not give any undertaking or incur any contractual obligation towards the class members, and moreover, the class members entrusted their personal information to Capital One, such that the provincial or federal legislation cannot apply to Amazon.

[135] Amazon adds that it did not make any representation or address any advertising whatsoever to the plaintiffs or the putative class members, and it argues that the information on its website addressed to Canadians in fact concerns only businesses, not natural persons.[54]

[136] But Amazon's website does not make this distinction. Its content is addressed to all Canadian consumers.

[137] Despite this, Amazon concludes that it also cannot be alleged to have committed an extracontractual fault towards the plaintiffs and the putative class members.

[138] Amazon is perhaps at the origin of this confidentiality incident, which may be inferred from the fact that the author of this intrusion is one of its former employees, who, while she was employed, was undoubtedly able to access all the data control, verification, and protection procedures as well as all the personal information that was supposed to be adequately protected.

[139] Amazon may have committed one or several faults, arguably incurring its contractual liability towards Capital One in the context of a possible action in warranty, but that is not the subject of the Court's analysis here.

[54] Exhibit R-6.

[140] In fact, there is little or no doubt that there will eventually be litigation between Amazon and Capital One, if it is not already the case, in the event that a class action is eventually authorized against Capital One.

[141] The Court notes that in the exhibits relied on by the plaintiffs, Capital One and Amazon have already, more than once, attributed ultimate liability for this unauthorized access to the other.

[142] The hypothesis of a contributory fault by each of these groups also cannot be excluded at this stage, as the plaintiffs appear to suggest.

[143] The issue now is whether as a result of its alleged faults and breaches, Amazon may incur direct liability to the putative class members to whom this personal information belongs.

[144] Amazon seeks to reduce and limit the scope of its undertakings that may arise from the representations it makes on its website[55] and the obligations that may be incumbent upon it depending on the provincial and federal statutes, and consequently, under article 1457 CCQ.

[145] Indeed, at first glance, Amazon's advertising and the information it publishes on the services it provides in Canada regarding the security of the storage of personal information that may be entrusted to it in the territory are not intended for Capital One, but rather for the putative class members and the public in general.

[146] The following are excerpts from Amazon's website intended for Canadian residents:

> The AWS Canada Region has two Availability Zones made up of one or more discrete data centers to help customers meet local compliance and security needs.
>
> …
>
> SECURITY AND COMPLIANCE
>
> Superior Cloud Protection
>
> At AWS, cloud security is our highest priority. As an AWS customer using cloud computing services
>
> In the Canada region, you will benefit from local servers and network architecture built to meet the requirements of the most security-sensitive organizations. AWS allows customers to scale and innovate, and provides the tools to maintain a protected environment. Customers can choose to secure their data locally, to help them meet Canadian PIPEDA regulations.

[55] *Ibid*.

[Emphasis added.]

[147] The undertakings set out therein are clear, precise, and as extensive as those set out in Capital One's documents, referred to above.

[148] It is therefore entirely conceivable, further to a preliminary examination of the statutory provisions in force in Quebec with respect to the protection of personal information, that Amazon could be considered a person who holds personal information belonging to the putative class members, despite the absence of a contractual relationship with them, and that Amazon has incurred statutory or legal liability towards those class members as a result.

[149] It is true that the allegations in the Application reveal that Amazon did not formally make any contractual undertaking to the plaintiffs or the putative class members; however, the Court remains unconvinced by Amazon's argument on the scope, in particular of the provincial statute, in its regard.

[150] As discussed above, the relevant statutory provisions of the Quebec *Act respecting the protection of personal information in the private sector* impose obligations on those who hold such information, without specifying or limiting those obligations to those who have entered into contracts for services with these cloud service enterprises, as opposed to the *CPA*, the application of which is limited to a merchant who has entered into a consumer contract with a consumer for a good or service.

[151] Section 3 of the Quebec *Act respecting the protection of personal information in the private sector* provides that a person who holds personal information on another "must take reasonable measures to reduce the risk of injury and to prevent new incidents of the same nature".

[152] Section 10 of the *Act* states:

> A person carrying on an enterprise must take the security measures necessary to ensure the protection of the personal information collected, used, communicated, kept or destroyed and that are reasonable given the sensitivity of the information, the purposes for which it is to be used, the quantity and distribution of the information and the medium on which it is stored.

[153] As a result of these provisions, it is plausible that Amazon may have a duty towards the plaintiffs and the putative class members, the violation of which may be akin to a statutory fault or an extracontractual fault under article 1457 CCQ reproduced above.

[154] It is therefore difficult for the Court at this stage to set aside the possibility that these provisions apply to Amazon, and limit their scope solely to Capital One, as Amazon suggests.

[155] According to Amazon, the provisions of the CCQ and especially those of the provincial statute on the protection of personal information cited above, concern only the principal person in charge or the administrator of the data collected or the person who controls it.

[156] Amazon submits that Capital One's liability under these specific statutes remains whole because it is the principal actor in the collection of this personal information.

[157] In this regard, it relies in particular on notices and communiqués issued by the Office of the Privacy Commissioner of Canada, neglecting the fact that the personal information of the members in this case were subsequently entrusted by Capital One to Amazon, as cloud services provider, to conclude that Capital One is solely liable for the information security breach concerning this personal information resulting from the unauthorized access.

[158] Thus, they argue that the cloud services provider, in this case Amazon, cannot incur any liability to the persons to whom this information belongs on the sole basis that it was Capital One who collected the information from the members.

[159] Amazon cites no Canadian court judgment or any other authority in support of this assertion.

[160] Indeed, the documents cited by Amazon during its arguments, which are essentially recommendations made by the Privacy Commissioner of Canada to businesses, organizations, and other persons who obtain personal information and entrust them to third persons, indicate that the person to whom the data is first entrusted remains responsible and bound by the obligation of information security, which seems perfectly conceivable and logical, but importantly, this is quite different from what Amazon argues because these notices and recommendations in no way suggest that a provider of hosting services like Amazon is not liable.

[161] In addition, the Application refers to a form of partnership[56] between Capital One and Amazon, in the context of which each of them could and can still derive commercial and financial benefits,[57] and pursuant to which Capital One must make available to Amazon the largest possible amount of its clients' personal information, even information older than that required for its operations, so that Amazon, using its own servers and software, can use other artificial intelligence tools to generate other information useful to its commercial operations and those of Capital One.

[162] In fact, Capital One and Amazon jointly presented the Cloud Custodian software to the public in 2016,[58] in particular on their respective websites.[59] This software was

---

56 Application at para. 10.20.
57 Application at para. 10.28.1.
58 At para. 10.31.8.
59 At para 10.30 and exhibit R-12.

intended to palliate or resolve the known or alleged vulnerability of Amazon's servers that were supposed to provide the desired protection.

[163] According to the allegations in the Application, Amazon even encouraged the massive migration of data collected by Capital One and kept by it until that time to Amazon's servers, as well as the implementation of the process known as Cloud Custodian,[60] designed and implemented together with Capital One, while reassuring Canadian consumers that their local servers and the architecture of their network would satisfy the requirements of organizations most sensitive to information security, to ultimately make available a protected environment to consumers choosing to use their local services (Canadians) and thereby satisfy the federal regulation of the protection of personal information.[61]

[164] In view of these allegations, it is not possible for the Court to minimize Amazon's role, as it suggests, and narrow the application and scope of the Quebec *Act respecting the protection of person information* and possibly of the *Federal Act* in its regard.

[165] There is therefore a real possibility that it will eventually be established that Amazon committed one or more extracontractual faults against Royer and the putative class members.

[166] In the alternative, Amazon refutes the plaintiffs' position that, in the event it is found extracontractually liable, which it vigorously denies, all the defendants in the proceeding could be found solidarily liable, alleging that the action directed against Capital One is contractual, while against Amazon it is extracontractual, such that solidarily among these two groups of defendants, other than mere *in solidum* liability, cannot be asserted under article 1525 CCQ.

[167] In this regard, the plaintiffs are trying to assimilate Amazon to Capital One or place them on the same footing vis-à-vis the class members, by invoking their common knowledge as of 2018 of their system's vulnerability and of the insufficiency of the means used to compensate for it, such as the Cloud Custodian.

[168] At first glance, the Court agrees with Amazon's argument that the facts alleged in the Application and the exhibits invoked in support thereof do not serve as indicia of the same type of legal relationship between the class members on the one hand, and Capital One and Amazon on the other.

[169] As a preliminary matter, it therefore seems possible to find that Amazon committed an extracontractual fault, but not that there is potential solidary liability among all the defendants resulting from the application to them of article 1525 CCQ having

---

60 At para 10.41 and exhibits R-8, R-9, and R-10.
61 Exhibit R-6, referring to the Federal *Act* cited at note 17.

regard to the provisions of the Quebec *Act respecting the protection of personal information* and the CCQ.

[170] The judge hearing the case on the merits can eventually assess and will have to determine the outcome of this potential solidarity, being mindful of the fact that Capital One cannot be found liable both contractually and extracontractually.[62]

False or misleading representations

[171] The Court would like to point out that the allegations in the Application, taken to be true at this stage of the proceeding, do not establish the possibility of an action based on false or misleading representations by the Amazon defendants towards the class members, as that notion is defined in the *CPA*, according to the same reasoning applied above to Capital One.

[172] The plaintiffs' allegations rely on the prohibition against prohibited practices under the *CPA*, which can result in the obligation to pay punitive damages under section 272 of the *Act*.

[173] First, and the Court considers this determinative, there is no allegation suggesting that a consumer contract, a contract of sale, of lease of goods, or of service may have been entered into by the plaintiffs and the class members on the one hand, and Amazon on the other.

[174] It could ultimately have been argued by the plaintiffs that Amazon may have incurred liability solely on the basis of a prohibited practice it committed, because in such case, the demonstration of a prohibited practice is not subordinate to the conclusion of a contract.[63]

[175] But the practice that is prohibited by the *CPA* consists of a merchant making false or misleading representations to a consumer for the purpose of entering into a consumer contract with the consumer, which cannot be the case for Amazon, whose services are intended solely for Capital One, even if they were ultimately for the benefit of Capital One's clients.

[176] Therefore, in the Court's view, it cannot validly be argued, even at the screening stage of the Application, that Amazon may have incurred its liability for false or misleading representations, as defined in the *CPA*, towards the plaintiffs or putative class members, because nothing shows or suggests that it entered into a consumer contract with the members or attempted to incite them to do so by means of a prohibited practice.

---

62 Article 1458 CCQ.
63 Section 217 *CPA*.

[177] Despite the plaintiffs' references to Amazon's website, it cannot be inferred from the allegations in their Application that Amazon wanted or sought to enter into a consumer contract directly with the class members.

[178] Accordingly, nothing in the Application on its face supports the theory that Amazon made false or misleading representations to the plaintiffs or the putative class members, or that the *CPA* applies to it, which must therefore be set aside in this case with respect to Amazon.

[179] In addition, as is also the case for Capital One, the plaintiffs allege no specific facts establishing the false or misleading nature of a representation made by Amazon, other than the occurrence of this intrusion into its personal information hosting system, which may in itself constitute an extracontractual or statutory fault, as discussed above, but that in no way establishes that the representations Amazon made on the protection and security measures it implemented were false.

(e) Pecuniary and non-pecuniary damages

[180] As for the damages of this nature that may be claimed, it should be recalled that a specific line of cases has developed in recent years with respect to the unauthorized access to personal information or the theft of personal information or identity. This case law may be interpreted as rather restrictive regarding the possibility of claiming such damages.

[181] The Court's examination of this case law indicates that the facts alleged in the application for authorization must reveal an arguable case and establish compensable injury at the authorization stage, such that the damages alleged must be more than ordinary inconvenience or the anxiety and fear that persons in such circumstances may experience. Uncertain, future, or hypothetical damages are not a compensable injury.

[182] In *Mustapha*,[64] an Ontario case, the Supreme Court first decided that injury compensable by damages must be more than psychological upset:

> [8] Generally, a plaintiff who suffers personal injury will be found to have suffered damage. Damage for purposes of this inquiry includes psychological injury. The distinction between physical and mental injury is elusive and arguably artificial in the context of tort. … :
>
> > In an age when medical knowledge is expanding fast, and psychiatric knowledge with it, it would not be sensible to commit the law to a distinction between physical and psychiatric injury, which may already seem somewhat artificial, and may soon be altogether outmoded. Nothing will be gained by treating them as different "kinds"

64 *Supra* note 10.

> of personal injury, so as to require the application of different tests in law. [Emphasis added.]
>
> [9] This said, psychological disturbance that rises to the level of personal injury must be distinguished from psychological upset. Personal injury at law connotes serious trauma or illness … The law does not recognize upset, disgust, anxiety, agitation or other mental states that fall short of injury. I would not purport to define compensable injury exhaustively, except to say that it must be serious and prolonged and rise above the ordinary annoyances, anxieties and fears that people living in society routinely, if sometimes reluctantly, accept. … Quite simply, minor and transient upsets do not constitute personal *injury*, and hence do not amount to damage.
>
> [Emphasis added; citations omitted.]

[183] Next, the Supreme Court explained that to be compensable, such injury must not be too remote:

> The remoteness inquiry depends not only upon the degree of probability required to meet the reasonable foreseeability requirement, but also upon whether or not the plaintiff is considered objectively or subjectively. One of the questions that arose in this case was whether, in judging whether the personal injury was foreseeable, one looks at a person of "ordinary fortitude" or at a particular plaintiff with his or her particular vulnerabilities. This question may be acute in claims for mental injury, since there is a wide variation in how particular people respond to particular stressors. The law has consistently held — albeit within the duty of care analysis — that the question is what a person of ordinary fortitude would suffer …

[184] This approach was followed in Quebec, in particular in *Li c. Equifax*:[65]

> [TRANSLATION]
>
> [26] Recall that the colour of right must be analyzed in light of the plaintiff's personal situation.
>
> [27] According to the allegations in the Amended application, the plaintiff was not the victim of identity theft and has not yet had to spend any money to purchase continuous credit monitoring services or suffered any trouble and inconvenience associated with the cancellation of credit cards and the organization of credit monitoring services, for example. The plaintiff describes future risk and expenses. He adds that he has suffered "mental distress". Is this sufficient? The Court does not think so. Here is why.
>
> [28] In *Zuckerman c. Target Corporation*, the Superior Court summarized the state of Quebec law on damages in such cases as follows:

[65] *Li c. Equifax*, 2019 QCCS 4340.

> [73] The Court concludes that the monitoring of bank accounts and credit cards constitute normal activities and not inconveniences for which the account or card holder can recover damages. However, other matters such as setting up credit monitoring and security alerts, obtaining credit reports, and cancelling cards or closing accounts and replacing them are not "ordinary annoyances, anxieties and fears that people living in society routinely, if sometimes reluctantly, accept" but may amount to something more. These are potentially matters for which class members would be entitled to compensation.
>
> [77] Zuckerman does not allege that he was the victim of fraud or identity theft. It is possible that he was the victim of fraud or identity theft and does not know it or that he will be the victim of fraud or identity theft in the future, but those possibilities seem increasingly remote with the passage of time.
>
> [78] Zuckerman cannot found the class action on damages that he did not suffer. He must allege that he suffered damages personally. Whether he can include in the class persons who suffered damages different from those that he suffered is a matter that the Court will consider, if it authorizes the class action, in the description of the class and the identification of the issues and the conclusions.

[29] These statements echo the concept that the risk of developing a future injury, such as a disease or infection, is not compensable damage in Quebec law. It is uncertain and hypothetical damage, prohibited under article 1611 CCQ and the relevant authorities on the matter. A risk is not an injury that is certain.

[30] In the circumstances, the plaintiff has no colour of right to the following damages:

- Economic loss resulting from the purchase of continuous credit monitoring services, among others; and
- Trouble and inconvenience associated with the cancellation of credit cards and the organization of credit monitoring services, among others.

[31] In addition, the "mental distress" alleged by the plaintiff is not characterized or described in a manner that exceeds the ordinary annoyances, anxieties and fears that people living in society routinely, if sometimes reluctantly, accept. More details would have been required, rather that mere allegations. According to the allegations in the Amended application, the Court finds that this injury alleged by the plaintiff is negligible and therefore has no colour of right.

[32] Last, there are no [TRANSLATION] "other losses" alleged by the plaintiff. There is therefore no colour of right in this respect.

> [33] The Court notes in conclusion that the plaintiff does not allege that he received a letter from the defendants informing him that he may have been affected by the hacking incident, as described in Exhibits D-1A, D-1B, and D-2.
>
> [34] The Court finds that the plaintiff did not establish compensatory damage in his personal case, which means that the class action has no colour of right and cannot be authorized in this regard. At this time, Quebec law does not recognize the mere fact that personal information is in the unauthorized possession of third persons, without more, as compensatory damage.
>
> [Citations omitted.]

[185] In addition, according to the defendants, this case can also be distinguished from other cases[66] in which compensable damage was established and in which, according to the evidence adduced, fraud resulting from the theft of data had been committed, which is not the case here, as evidenced by the results of the inquiry held before a US criminal court on the facts and acts committed by Paige A. Thompson, which found that she did not or could not have used this unlawfully obtained data.

[186] Accordingly, the defendants submit that to obtain pecuniary compensatory damages, the plaintiffs must establish that such damages can be assessed or quantified, such that the Court should not consider the risk of future injury, even if it is alleged, because it cannot lawfully be compensated under Quebec law.[67]

[187] Essentially, the facts giving rise to a cause of action alleged by the plaintiffs in this case are limited to this unlawful and unauthorized access by Paige A. Thompson on March 22 and 23, 2019, with respect to which the inquiry revealed that, although she admitted the acts alleged against her, she did not disclose the personal information obtained to anyone or use it in any manner.

[188] There is no specific allegation in the Application, not even in its fourth amended version, of the occurrence of identity theft or any difficulty arising from this unauthorized access that could have resulted in expenses for the plaintiffs or any steps taken or disbursements made following the unlawful use or theft of personal information since the events that occurred in March 2019.

[189] Of course, we cannot set aside the fear of the risk that another access will occur, or could have occurred since 2019 and that personal information was stolen and distributed, but not yet used. Once again, however, this consists of speculation and hypotheses.

---

[66] See e.g., *Mazzona c. Daimler Chrysler Financial services canada inc.,* 2012 QCCS 958.
[67] Articles 1611 and 1613 CCQ.

[190] According to the defendants, there is therefore no future, direct, and foreseeable injury,[68] because the injury invoked is not only hypothetical and uncertain, but also improbable, and it is difficult, even impossible, to assess.

[191] The plaintiffs claim that the total value of their patrimonies and that of the class members have been negatively affected by this unauthorized access of their personal information. The same is true for their credit scores. They also claim that the membership fees for this credit card have become too high because they are not justified.

[192] In support of their claims, the plaintiffs invoke the statistics obtained by the Office of the Privacy Commissioner of Canada[69] and from studies and surveys conducted in Canada and the United States, in particular regarding the theft of social insurance numbers.[70]

[193] In addition to the fact that this access currently seems to have had no tangible effect, the Court considers it quite difficult, even impossible, on the basis of the evidence presented to it, to assess a loss of value of this information or a loss corresponding to the reduction in value of the services offered or the risks associated with anticipated eventual difficulties when making future credit applications.

[194] Last, the plaintiffs seek compensation for the injury arising from the defendants' lack of diligence to minimize the possible consequences of this unauthorized access. They fault Capital One for having waited until July 29, 2019, to inform the public in a communiqué that this confidentiality incident had occurred four months earlier and claim that Capital One may have been informed of this incident before July 17, 2019.

[195] Nothing is alleged by the plaintiffs on the actual impact of such delay, because at the time of Paige A. Thomson's arrest on August 28, 2019, she had not yet used or reproduced the personal information obtained, nor had she been able to sell or distribute it.

[196] However, the Court is of the view that the issue of monitoring costs requires a different approach.

[197] Indeed, it seems necessary to make a distinction here, as this Court did in *Zuckerman c. Target Corporation*, referred to above, between random or ad hoc, or even frequent and regular verifications of their clients' bank accounts and statements that financial institutions may conduct for the purposes of preventing and monitoring fraud, even in the absence of a confidentiality incident, like the one that occurred in this case, because these acts are part of the day-to-day operations of financial institutions and the banking services they generally provide to all theirs clients at no additional charge, and the verification and monitoring of clients' accounts and statements following an intrusion,

---

68 Articles 1611 and 1613 CCQ.
69 Application at para 10.73.5 *et seq*.
70 *Ibid.* and para.10.73.7 *et seq*.

which services form part of Capital One's specific offer for a period of two years at no charge, even though the evidence adduced in this case does not allow us to make a particular distinction regarding the nature of the verifications conducted.

[198] In addition, the verification and monitoring services offered at no charge in this case do not arise from the use of data, the theft of personal information, or fraud, but solely from the occurrence of the confidentiality incident itself and the risks it entails, despite the absence of known consequences in view of the results of the inquiry concerning the acts of Paige A. Thompson.

[199] Also, by the fact of its offer to provide verification and monitoring services, and regardless of the sufficiency of that offer, Capital One seems to recognize, to some extent, that it is a special situation that requires such monitoring of its clients' accounts and statements.

[200] The plaintiffs allege that this two-year period during which they can benefit from such verification and monitoring services at no charge is clearly insufficient. According to them, in matters involving the theft of personal information, a person can never truly be protected from fraud despite the passage of time, and they invoke several emails received from putative class members to this effect.

[201] There is therefore only one remaining question, that is, the sufficiency of this two-year period because it seems clear that this verification and monitoring process is necessary, or at least useful, and that it arises directly from this confidentiality incident.

[202] Indeed, it may be an inconvenience that is more than ordinary, which the judge hearing the merits will have to assess, that may extend over a period longer than two years, and that may also result in a disbursement of money.

[203] It may even be suggested that this two-year period is a standard that is known, recognized, and followed by those in the industry, and accordingly, ultimately just as known by those malicious and ill-intentioned persons who simply wait for that two-year period known in the industry to elapse before perpetrating their wrongdoing.

[204] In *Zucherman c. Target Corporation*,[71] Hamilton J., now of the Court of Appeal, preferred to leave for the trial judge the issue of determining whether an expense of $19.95 made by a representative for the costs of monitoring his account could be considered a compensable injury.

[205] In *Lévy c. Nissan*,[72] the Court of Appeal upheld the judgment of the Superior Court finding, as Hamilton J. did, that it was more appropriate for the trial judge to

---

71 2021 QCCA 682.
72 *Ibid*.

determine the possibility of claiming the cost of monitoring bank accounts, giving the plaintiff the benefit of the doubt.

[206] More recently, this Court authorized a class action in which there was no allegation of data theft, but only stress, fear, and anxiety, in particular because the data had been made public.

[207] The cost of monitoring bank accounts was claimed on the ground that the period of one year offered at no charge was insufficient,[73] and authorization to institute a class action was granted.

[208] At the time of the hearing, this two-year period of monitoring at no charge had presumably expired, and it had probably expired at the time of the fourth amendment to the Application on April 25, 2022, even if that amendment did not allege that the plaintiffs or the class members had to pay amounts of money to extend this verification and monitoring period.

[209] Accordingly, the Court intends to recognize only this head of damage as appearing compensable at the authorization stage, also leaving for the trial judge full latitude, with all the evidence that will be adduced before him or her, to ultimately decide whether additional costs for a verification and monitoring period that is longer that the two years offered in this case may constitute compensable injury because they are reasonably foreseeable and arise directly from the defendants' fault.

[210] Thus, except for these additional verification and monitoring costs for a period greater than two years, the plaintiffs have not established the existence of any other pecuniary or non-pecuniary injury suffered to this day akin to costs incurred or financial losses actually suffered, or even future financial losses or expenses that are also reasonably foreseeable.

(f) Punitive damages

[211] The plaintiffs also claim punitive damages and rely for this purpose on both section 49 of the *Charter*, invoking an intentional interference with their right to the protection of their privacy, and section 272 *CPA.*

[212] As discussed above, the case law requires that the intention of the wrongdoers be proven such that sufficiently clear and precise allegations in this regard must be made in the Application.

[213] The plaintiffs do not allege any precise fact establishing that they were the subject of a specific intentional violation by the defendants of their right and that of the class members to the protection of their privacy under section 5 of the *Charter*, cited above.

---

[73] *Zucherman c*. *MGM Resorts International*, 2022 QCCS 2914.

[214] Rather, the Application faults Capital One for its negligent conduct and lack of concern for the security of the personal information it obtained from its clients, while it knew or should have known, during the migration of this substantial amount of personal information in 2015, that the protection and security of this data could be affected and eventually compromised because the measures implemented were inadequate and insufficient.

[215] According to the plaintiffs, Capital One did not comply with industry standards and practices regarding information security and placed little importance on the protection and security of its clients' personal information.

[216] It favoured its potentially lucrative association with Amazon, while keeping too much data for that purpose, including that of members whose credit had been refused, over too long a period, and went forward with this massive migration of the personal information of its clients to a public hosting site known to be less secure, was late informing the members of this confidentiality incident, and failed to fix the vulnerability of the protection and security measures implemented.

[217] According to author Mtre Claude Dallaire, who has since become a judge of this Court, a reading of the case law on the intentional interference with a right or freedom recognized by the *Charter* reveals that it is possible to infer such intentional interference from the conduct of a reasonable person who, acting as such, cannot ignore the natural and immediate consequences that his or her acts will cause:

> [TRANSLATION]
>
> The intention is what can be deduced from the actions of the person who committed the interference. If the conduct is shocking, unreasonable, unjustified, serious, or repetitive, there is a good chance that there will be elements present to meet the burden of proof required by the Supreme Court.[74]

[218] Relying on a judgment of the Supreme Court, the author goes on to state that a complainant has the burden of proving that the party in question acted intentionally, maliciously, or vexatiously, or that the complainant's conduct can be characterized as severe ignorance, carelessness, or neglect, reaching the level of seriousness to be considered a fault:[75]

> [TRANSLATION]
>
> In *Gauthier c*. *Corporation municipale de Ville de Lac Brôme*, virtually all indicators were considered by the Supreme Court to allow it to conclude that it was not possible for a reasonable person acting as such to be unaware of the natural and

---

[74] *Supra* note 24.
[75] *Ibid*.

> immediate consequences that his or her actions would cause or that he or she did not intend such interference with the integrity and dignity of the victim.
>
> According to our understanding, the Court used the test of [TRANSLATION] "knew or should have known" to establish the intention of the various persons who committed the interference, in particular that of the employer city. …
>
> In light of these examples, we note that it is not difficult to meet the burden of proof required to award exemplary damages under the Quebec *Charter*. It is simply necessary to understand what the intention referred to in section 49(2) is. The intention is what can be deduced from the actions of the person who committed the interference. If the conduct is shocking, unreasonable, unjustified, serious, or repetitive, there is a good chance that there will be elements present to meet the burden of proof required by the Supreme Court.[76]

[219] The Court of Appeal and this Court have applied these teachings of the Supreme Court:

> [30] The notion of intentional interference requires more than simple negligence but is not as strict as a specific intent. In one of the landmark cases on the topic, the Supreme Court stated the following:
>
> > 121. Consequently, there will be unlawful and intentional interference within the meaning of the second paragraph of s. 49 of the *Charter* when the person who commits the unlawful interference has a state of mind that implies a desire or intent to cause the consequences of his or her wrongful conduct, or when that person acts with full knowledge of the immediate and natural or at least extremely probable consequences that his or her conduct will cause. This test is not as strict as specific intent, but it does go beyond simple negligence. Thus, an individual's recklessness, however wild and foolhardy, as to the consequences of his or her wrongful acts will not in itself satisfy this test.
>
> [31] The judge concluded that the Application does not provide allegations to the effect that Respondent intentionally intended to expose its customers to a data breach. He pointed out that if Respondent had indeed been careless or committed gross negligence, it did not act deliberately to harm its customers.
>
> [32] The judge's reasoning fails to acknowledge that an intentional interference can arise not only when the author of the negligence wishes to cause the consequence of the wrongful interference but also when a "person acts with full knowledge of the immediate and natural or at least extremely probable consequences that his or her conduct will cause", which is more likely to be the case here.[77]
>
> [Emphasis added; citations omitted.]

---

[76] *Ibid*.
[77] *Supra* note 25.

[220] In a case involving several faults that were to some extent comparable to those invoked in this case, although based on different facts, this Court found:[78]

> [64]The second paragraph of section 49 of the Charter authorizes the award of punitive damages where the unlawful interference with rights or freedoms protected by the Charter is intentional.
>
> [65] The case law requires proof:
>
> > (i) that the author of the interference wished to cause the consequences of the wrongful interference, or
> >
> > (ii) that he or she was aware of the immediate and natural or extremely probable consequences of his or her misconduct.
>
> [66] The notion of intentional inference requires more than simple negligence but is not as strict as a specific intent.
>
> [67] The claim for punitive damages can stand alone, even in the absence of compensatory damages.
>
> [68] The allegations of the Application for authorization supporting the claim for punitive damages are the following:
>
> 48. In fact, without limiting the generality of the foregoing, Defendant was grossly negligent and/or intentionally negligent when it:
>
> a. did not follow or properly implement an effective data security industry standard to protect the Class Members' personal information, which information MGM allowed to be accessed and downloaded from an external cloud server by unauthorized parties;
>
> b. tried to downplay and hide the magnitude of the Data Breach for almost 1 year;
>
> c. failed to promptly notify the Plaintiff and the Class Members of the Data Breach for almost one year, which in and of itself is abusive and egregious, justifying an award for such punitive damages;
>
> d. failed to properly ensure that Plaintiff and Class Members are protected by credit monitoring services by both Equifax Canada and TransUnion and failing to post fraud alerts on the Class Members' credit files immediately after the Data Breach;
>
> e. waited until after the media has exposed the fact that the personal information of millions of MGM clients was published on a hacking forum before notifying the Class Members, the whole as reported in the R-2 articles;

[78] *Zucherman c. MGM Resorts International*, 2022 QCCS 2914.

> f. failed to provide assistance and relevant information about the Data Breach on its websites;
>
> g. failed to even provide a telephone number for Class Members to call in order to access information about the Data Breach. […]

[221] According to these judgments, the Court may draw inferences on the basis of the negligent and reckless conduct alleged by the complainant to conclude that the other party's attitude was reprehensible with respect to the confidentiality of the personal information thus rendered accessible.

[222] Ultimately, and especially at this stage of the proceeding, the Court must assess whether the factual background, described in great detail in the Application in this case, shows conduct that transcends the event that occurred in March 2019 and is merely its culmination, and may seriously trouble, even shock, a reader of this account who is reasonably aware and informed, while being neutral and independent.

[223] According to the Application, the conduct in this case involves first the colossal amount of data involved, some of which had become useless and should possibly have been quickly destroyed, and some which was kept for too long.

[224] According to the Court, beyond the fault committed, the conduct must also indicate a reckless attitude and conduct by Capital One, nonchalant and insensitive to the importance of the protection of privacy during this migration of personal information in 2015, all the while having full knowledge of the risk that the result could be a breach of confidentiality and serious consequences, such as the theft of personal information in this case, in view of the notices published, sanctions obtained, and warnings issued.

[225] This conduct may be even more shocking if the party in question is more focused on the commercial and financial interest that may come from the use of this personal information, which may be inferred in this case from the lack of diligence and remedial measures for the future once the confidentiality incident and its cause were known, and although the deficiency seemed obvious, by both Capital One and Amazon, who mutually accuse each other of having caused the incident.

[226] The Application alleges that Capital One and Amazon continued to follow the same procedures and measures as those in place since the migration of data to Amazon, after the incident that occurred in March 2019, without correcting their deficiencies.[79] The plaintiffs' allegations cannot be characterized as hypothetical or speculative, and in fact, they are not contested.

[227] Indeed, the Application alleges that Capital One and Amazon did nothing, although alerted by various persons in the industry, which will have to be proven, to

---

[79] Application at para. 10.59.

prevent the March 2019 incident from occurring, to counter it, or to avoid it happening again in the future.

[228] This assessment must also take into account the legitimate expectations of the class members towards a major financial institution, the reputation of which is often measured against its discretion, reserve, prudence, and its absolute compliance with confidentiality.

[229] This is the conduct revealed, at least on a *prima facie* basis, by Capital One, with whom the class members dealt with, such that in the Court's view, the allegations in the Application may give rise to an award to the class members of punitive damages payable by Capital One under sections 5 and 49 of the *Charter*.

[230] However, the Court cannot draw such conclusions on Amazon's conduct in this case due to its particular situation vis-à-vis the class members.

[231] Indeed, Amazon certainly made public representations on the protection of personal information and respect for privacy in Canada pursuant to the legislation applicable to it, but it is not the one who sought out this clientele, contracted with the members, or collected this personal information from them.

[232] According to the information available on its website, Amazon is a service business that offers personal information hosting to the public.

[233] Its conduct in this case cannot be analyzed using the same standards as those considered generally applicable to a financial institution like Capital One.

[234] As for the application of section 272 *CPA*, the defendants rightly submit that the plaintiffs do not meet the fourth criterion of the analytical framework regarding the application of the *CPA* set out by the Supreme Court in *Richard v. Time Inc.*,[80] discussed above, due to the absence of false or misleading representations in this case.

(g) The Court's conclusions on article 575(2) CCP

[235] The Court is of the view that the plaintiff Abou-Khadra did not establish that he has an arguable case to assert against the defendants in this matter.

[236] However, the Court finds that the plaintiff Royer established the existence of such an arguable case to assert against all the defendants, by him and by all the putative class members residing in Quebec who were informed of the incident that occurred on March 22 and 23, 2019, that is, a contractual fault by Capital One, and an extracontractual fault by Amazon, for pecuniary damages consisting of the costs of verifying and monitoring the class members' Capital One accounts and statements, for a period greater than two years, to be determined by the Court.

---

[80] 2012 SCC 8.

[237] That said, this cause of action cannot extend to all the damages claimed, which must be limited, like the issues common to all the class members, to the foreseeable costs of verifying and monitoring their accounts and statements, to which may be added, for the Capital One group defendants, punitive damages under section 49 of the *Charter* to be determined by the Court.

[238] Last, the Application puts forward a conclusion to be set out in the proposed class action requiring the defendants to implement adequate protection and information security measures to prevent the occurrence of another unauthorized access.

[239] The manner in which this injunctive conclusion sought by Royer is currently worded is much too vague, imprecise, and general for it to be capable of eventually being executed, knowing the consequences that the violation of a court order may entail.

[240] The Court does not dismiss it at this stage, however, preferring instead to invite the plaintiff Royer to reformulate it in his originating Application to eventually be filed and notified further to this judgment if he still wishes to propose this particular debate.

III. The criterion set out in article 575(4) CCP: are the class members appointed as representative plaintiffs in a position to properly represent the putative class members?

[241] In this regard, Amazon reiterates that neither the plaintiff Royer, nor the plaintiff Abou-Khadra have an arguable cause of action to assert against it because they have no legal relationship with Amazon, and the Application contains no allegation or evidence of compensable injury against the defendants.

[242] The Court is of the view that the plaintiff Royer has established that he has an arguable cause of action to assert against all the defendants, and with respect to Amazon, on an extracontractual basis and in light of the possible application of the Quebec *Act respecting the protection of personal information in the private sector* to it.

[243] Accordingly, for the reasons set out in greater detail above, the Court is of the view that only the plaintiff Michael Royer appears to be in a position to properly represent the putative class members because, contrary to the plaintiff Abou-Khadra, he is one of the 6,000,000 Canadian residents informed of an unauthorized access of his personal information.

3. CONCLUSION

FOR THESE REASONS, THE COURT:

[244] **GRANTS** the plaintiff Michael Royer's application for authorization to institute a class action against the defendants Capital One Bank (Canada Branch), Capital (Financial Corporation), and Capital One Bank (USA) National Association, and against

the defendants Amazon.com Inc., Amazon.com.ca Inc., Amazon Web Services Canada Inc., Amazon Web Services Inc., and Amazon Technologies Inc.;

[245] **DISMISSES** the application for authorization to institute a class action filed by the plaintiff Ala'a Abou Khadra against all the defendants;

[246] **DESCRIBES** the Class of members as follows:

> [TRANSLATION]
>
> All persons, entities, or organizations residing in Quebec who had a credit card issued by Capital One or applied to obtain one and whose personal information were subject to unauthorized access on March 22 and 23, 2019.

[247] **DESIGNATES** the plaintiff Michael Royer as representative of the members of the Class;

[248] **IDENTIFIES** the common issues to be debated in the class action as follows:

(a) Did the Capital One group defendants commit faults against the Class members under the contract binding the parties with respect to the protection and security of their personal information since 2004, during the migration of their personal information to the defendant Amazon's servers in 2015 and subsequently to that?

(b) Does the *Personal Information Protection and Electronic Documents Act* apply to the defendants?

(c) Did the Capital One group defendants and the Amazon group defendants commit faults against the Class members pursuant to the *Act respecting the protection of personal information in the private sector* and the *Personal Information Protection and Electronic Documents Act* between 2004 and the date of these proceedings?

(d) Are the Capital One group defendants and the Amazon group defendants liable to pay the Class members the costs of monitoring their Capital One credit card accounts and statements for a period greater than two years, and if so, what costs may be claimed?

(e) Did the Capital One group defendants interfere with the Class members' right to privacy under the *Charter of human rights and freedoms*?

(f) Are the Capital One group defendants liable for punitive damages to the Class members, and if so, in what amount?

[249] **IDENTIFIES** the conclusions sought as follows:

- **GRANT** the class action instituted by the plaintiff Michael Royer against all the defendants;

- **DECLARE** that the defendants Capital One Bank (Canada Branch), Capital (Financial Corporation), and Capital One Bank (USA) National Association committed one or several contractual faults against the Class members;

- **DECLARE** that the defendants Capital One Bank (Canada Branch), Capital (Financial Corporation), and Capital One Bank (USA) National Association, Amazon.com Inc., Amazon.com.ca Inc., Amazon Web Services Canada Inc., Amazon Web Services Inc., and Amazon Technologies Inc. infringed the *Act respecting the protection of personal information in the private sector* and the *Personal Information Protection and Electronic Documents Act*;

- **DETERMINE** the amount of the costs required to monitor the credit card accounts and statements of the Class members, for a reasonably foreseeable period, as a consequence of the events that occurred on March 22 and 23, 2019, and **CONDEMN** the defendants solidarily to pay the Class members the amount of these costs;

- **DECLARE** that the defendants Capital One Bank (Canada Branch), Capital (Financial Corporation), and Capital One Bank (USA) National Association, interfered with the Class members' right to privacy guaranteed by section 5 of the *Charter of human rights and freedoms*, and **CONDEMN** them solidarily to pay the Class members an amount to be determined by the Court as punitive damages under section 49 of the *Charter of human rights and freedoms*, with interest at the legal rate and the additional indemnity provided by law;

- **ORDER** the collective recovery of the Class members' claims, or failing that, the individual recovery of said claims;

- **THE WHOLE** with costs against the defendants, including all expert costs and the costs of publishing the notices required by law;

[250] **DECLARES** that unless they have opted out, all Class members will be bound by any judgment rendered on the class action, in the manner provided by law;

[251] **FIXES** the period during which a Class member may request to opt out at thirty (30) days following the date of the notice to Class members, following which all Class members who have not asked to opt out will be bound by the judgment to be rendered on the class action;

[252] **ORDERS** the publication of a notice to Class members of this class action that is accessible to the Class, drafted in the appropriate manner in accordance with article 579 CCP;

[253] **ORDERS** the defendants to send the notice to the Class members at their last known email address with the words [TRANSLATION] “Notice of class action” in the subject line of the email;

[254] **ORDERS** the defendants to publish the notice to the Class members on their website, their Facebook or Threads page, and their Twitter page, with the words [TRANSLATION] “Notice of class action” for thirty (30) days following the date of publication of the notice;

[255] **ORDERS** that the closing date of the Class will be the date of the publication of the notice to Class members;

[256] **THE WHOLE**, with legal costs against the defendants.

_____

BERNARD TREMBLAY, J.S.C.

Mtre Jeff Orenstein
Mtre Andrea Grass
CONSUMER LAW GROUP INC.
Counsel for the plaintiffs

Mtre Noah Boudreau
Mtre Mirna Kaddis
FASKEN MARTINEAU DUMOULIN INC.
Counsel for the defendants Capital One Bank (Canada Branch), Capital (Financial Corporation), and Capital One Bank (USA) National Association.

Mtre Paule Hamelin
GOWLING WLG (CANADA)
Counsel for the defendants Amazon.com Inc., Amazon.com.ca Inc., Amazon Web Services Canada Inc., Amazon Web Services Inc., and Amazon Technologies Inc.

Dates of hearing: January 31 and February 1, 2023