

# COUR SUPÉRIEURE

CANADA  
PROVINCE DE QUÉBEC  
DISTRICT DE MONTRÉAL

N° : 500-06-001010-194

DATE : 1<sup>er</sup> août 2023

---

**SOUS LA PRÉSIDENTE DE L'HONORABLE BERNARD TREMBLAY, j.c.s.**

---

**MICHAEL ROYER  
ALA'A ABOU-KHADRA**

Demandeurs

c.

**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.**

Défenderesses

---

**JUGEMENT**  
**(sur une demande d'autorisation d'exercer une action collective)**

---

## TABLE DES MATIÈRES

1. CONTEXTE.....	2
2. ANALYSE.....	4
I. Les questions en litige.....	4
II. Le critère prévu à l'article 575 al. 2 C.p.c. : les demandeurs ont-ils chacun une cause défendable à faire valoir à l'encontre des défenderesses?.....	7
a) Le droit applicable au débat.....	7
b) Le demandeur Abou-Khadra.....	21
c) Capital One.....	22
La faute.....	22
Les représentations fausses ou trompeuses.....	30
d) Amazon.....	31
La faute.....	31
Les représentations fausses ou trompeuses.....	36
e) Les dommages pécuniaires et non pécuniaires.....	37
f) Les dommages punitifs.....	44
g) Conclusions du Tribunal sur l'article 575 al. 1 par. 2 C.p.c.....	49
III. Le critère prévu à l'article 575 al. 4 C.p.c. : les membres auxquels les demandeurs entendent attribuer le statut de représentants sont-ils en mesure d'assurer une représentation adéquate des membres putatifs?.....	50
3. CONCLUSION.....	50

### 1. CONTEXTE

[1] La *Demande pour autorisation d'exercer une action collective* [la Demande] invoque la survenance, les 22 et 23 mars 2019, d'un incident de confidentialité qui interpelle et inquiète tout citoyen qui accepte de confier quotidiennement ses renseignements personnels à de très nombreux acteurs de l'activité humaine.

[2] La Demande est introduite par Michael Royer [Royer] le 30 juillet 2019.

[3] Elle est dirigée contre les sociétés Capital One Bank (Canada Branch), Capital One Financial Corporation et Capital One Bank (USA) National Association [Capital One

ou les défenderesses du groupe Capital One ou Capital One], formant l'une des plus importantes institutions financières en Amérique du Nord.

[4] Le demandeur Ala'a Abou-Khadra [Abou-Khadra] s'ajoute à la Demande à l'occasion d'une modification subséquente de celle-ci<sup>1</sup>, ainsi que les défenderesses Amazon.com inc., Amazon.com.ca inc., Amazon Web Services Canada inc., Amazon Web Services inc. et Amazon Technologies inc. [Amazon ou les défenderesses du groupe Amazon], un géant reconnu du commerce électronique qui a fourni à Capital One l'espace infonuagique permettant le stockage d'une imposante quantité de renseignements personnels.

[5] Cet incident cybernétique, ainsi qualifié par les demandeurs, consiste en un accès non autorisé par une ancienne employée d'Amazon, Paige A. Thompson, aux renseignements personnels détenus par cette entreprise, initialement recueillis par Capital One et appartenant à environ 6 000 000 de résidents canadiens et à 100 000 000 de résidents américains.

[6] Le déroulement de cette instance a été ponctué de quatre modifications de la Demande qui compte maintenant plus de 250 paragraphes, suivies de demandes des défenderesses donnant lieu à des jugements interlocutoires pour la production d'éléments de preuve additionnels visant à contrer ou à compléter certaines allégations de la Demande, ainsi que par des requêtes des demandeurs pour obtenir l'autorisation de tenir des interrogatoires préalables écrits.

[7] Un grand nombre de documents ont également été produits par les demandeurs pour décrire, avec moult détails, le contexte historique et technologique de cette intrusion dans le système d'Amazon.

[8] Ces documents émanent surtout d'autres dossiers judiciaires dans lesquels furent introduites des actions collectives similaires et demeurant actives au Canada, ainsi qu'aux États-Unis mais qui ont été réglées hors Cour depuis dans ce dernier cas<sup>2</sup>.

[9] Ces documents comprennent notamment la transcription intégrale de l'enquête criminelle tenue à la suite des accusations portées aux États-Unis par le FBI contre Paige A. Thomson, ainsi que certains éléments de preuve produits dans le cadre de cette enquête.

[10] Une demande en certification d'une action collective déposée en Ontario par Rina Del Giudice & Daniel Wood, basée sur les mêmes événements qu'en l'espèce, dirigée contre les défenderesses du groupe Capital One et les défenderesses du groupe

---

<sup>1</sup> 29 janvier 2020.

<sup>2</sup> Par. 10.74 et suivants de la Demande.

Amazon, comme c'est également le cas en la présente instance, a été rejetée le 4 août 2021 par l'honorable juge Paul M. Perell de la Cour supérieure de justice de l'Ontario<sup>3</sup>.

[11] Des enjeux de nature procédurale et autres de cette nature semblent avoir été déterminants dans cette affaire.

[12] Une autre demande en certification d'une action collective dirigée contre les défenderesses du Groupe Capital One seulement, a été déposée en Colombie-Britannique par *Duncan Campbell*.

[13] Cette demande est basée sur les mêmes événements que ceux invoqués dans le présent dossier et la certification de l'action collective fut accordée le 3 juin 2022 par l'honorable juge Nitya Iyer de la Cour suprême de la Colombie-Britannique<sup>4</sup>.

[14] Même si leur lecture peut s'avérer fort instructive et inspirante pour le soussigné, ces deux jugements, bien que rendus au Canada, ne peuvent être invoqués en la présente instance comme ayant acquis l'autorité de la chose jugée puisque rendus dans d'autres juridictions et parce qu'elles impliquent des plaignants différents.

[15] Ces jugements ne lient pas davantage le Tribunal sur le droit applicable dans le présent dossier, même si les plaignants possèdent une cause d'action similaire à celle des demandeurs en l'espèce, car ces jugements en certification ont été rendus en application de principes juridiques différents, tant en matière de certification d'action collective qu'en matière de responsabilité civile, et que ces principes sont issus de dispositions législatives distinctes, ainsi que de la *common law*, et ne sont pas applicables au Québec.

## 2. ANALYSE

### I. Les questions en litige

[16] Les demandeurs soutiennent que les défenderesses du groupe Capital One et du groupe Amazon doivent les indemniser, solidairement, pour le préjudice qu'ils ont subi, à l'instar de tous les membres putatifs du groupe identifiés par les demandeurs et désignés comme étant:

“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;”

<sup>3</sup> *Del Giudice v. Thompson*, 2021 ONSC 5379.

<sup>4</sup> *Campbell v. Capital One Financial Corporation*, 2022 BCSC 928.

[17] Dans les conclusions de leur Demande, les demandeurs identifient douze (12) questions de fait et de droit qu'ils considèrent communes aux membres putatifs et qui devraient être débattues devant le Tribunal, afin que celui-ci détermine, dans le cadre de l'action collective projetée, si les défenderesses sont ou non responsables des dommages qu'ils réclament.

[18] Essentiellement, ils reprochent aux défenderesses d'avoir fait preuve de négligence, d'abord en ayant failli à leurs obligations de protéger adéquatement les renseignements personnels qu'elles ont recueillis auprès d'eux et des membres putatifs sur une période de plusieurs années, d'avoir conservé trop longtemps ces renseignements, incluant ceux de membres dont la demande de crédit avait pourtant été refusée, et puis d'avoir fait défaut d'héberger ces renseignements au sein d'un environnement sécuritaire au plan informationnel et adéquatement protégé contre les intrusions.

[19] Plus spécifiquement, les demandeurs, qui sont titulaires chacun depuis plusieurs années d'une carte de crédit Costco émise par Capital One, blâment les défenderesses du groupe Capital One d'avoir effectué vers l'année 2015, la migration des renseignements personnels appartenant à leurs très nombreux clients et qui sont conservés sur leurs serveurs, vers un site d'hébergement moins sécuritaire, public et exploité commercialement par les défenderesses du groupe Amazon, permettant ainsi à Paige A. Thompson d'avoir accès à un nombre colossal de renseignements personnels leur appartenant.

[20] Les demandeurs incriminent également les défenderesses parce qu'elles n'auraient pas pris les mesures et les moyens pour prévenir cet accès non autorisé, et qu'elles auraient tardé à le découvrir, puis d'en informer les membres, et enfin, d'avoir fait défaut de ne pas corriger par la suite la problématique à l'origine de cette intrusion à ces fort nombreux renseignements personnels.

[21] Le demandeur Abou-Khadra allègue au surplus que sa carte de crédit a été débitée du montant de deux transactions qu'il n'a pas lui-même effectuées, ni autorisées.

[22] À l'instar des parties qui n'ont pas insisté sur ce point, ni présenté de preuve spécifique à cet égard, le Tribunal n'entend pas faire de distinction dans l'analyse qui va suivre, sur la responsabilité particulière pouvant incomber à l'une ou l'autre des défenderesses du groupe Capital One par rapport aux autres défenderesses de ce groupe, ni, de la même manière, sur la responsabilité particulière pouvant incomber à l'une ou l'autre des défenderesses du groupe Amazon par rapport aux autres défenderesses de ce groupe.

[23] Le Tribunal entend donc s'attarder sur les distinctions pouvant exister entre le recours envisagé par les demandeurs contre les défenderesses du groupe Capital One, et celui qu'ils veulent tenter contre les défenderesses du groupe Amazon, alors qu'il

n'existe pas de relations contractuelles entre les défenderesses du groupe Amazon et les demandeurs, ni les membres putatifs dans la présente affaire.

[24] Fait à souligner, les demandeurs formulent dans leur Demande une conclusion de nature injonctive contre les défenderesses, afin qu'il leur soit enjoint d'établir et de mettre en place des mesures adéquates de protection et de sécurité pour prévenir et détecter tout accès non autorisé aux renseignements personnels qu'elles détiennent.

[25] Étant formulée en des termes très larges et imprécis, cette conclusion n'est vraisemblablement pas susceptible d'exécution en nature ou forcée, et encore moins susceptible de sanction par la voie d'une possible condamnation pour outrage au Tribunal, de sorte que cette conclusion ne peut, à elle seule, assurer la viabilité, ou à tout le moins, le maintien de l'action collective proposée au stade de l'autorisation, cela dans l'éventualité où le Tribunal en venait à la conclusion qu'à l'égard des dommages réclamés, les demandeurs n'auraient pas satisfait au deuxième critère prévu à l'article 575 C.p.c.

[26] Les dommages réclamés par les demandeurs comportent onze (11) chefs distincts et sont décrits au paragraphe 6 de la Demande.

[27] Ils sont de trois ordres : pécuniaires, non pécuniaires et punitifs.

[28] D'une part, les demandeurs réclament des dommages pécuniaires, non quantifiés et pour la plupart, essentiellement à prévoir ou à anticiper, pour eux-mêmes et pour tous les membres putatifs, dont la perte de la valeur patrimoniale de leurs renseignements personnels et qui découle de cette atteinte à leur caractère privé, ainsi que les coûts d'adhésion trop élevés pour les services offerts par Capital One et obtenus de celle-ci en ce qu'ils ne répondent plus à leurs représentations sur le plan de la sécurité informationnelle.

[29] Ils réclament aussi, à ce titre, les coûts qu'ils devront engager pour assurer une vérification et une surveillance régulières de leurs comptes et relevés, sur une plus longue période de temps que celle de deux (2) ans durant laquelle de tels services leur ont été offerts gratuitement par Capital One, ainsi que les coûts qu'ils devront engager afin de faire face à une éventuelle fraude résultant d'un vol de leur identité dont les coûts nécessaires pour identifier et mettre sous les verrous l'auteur d'une telle fraude, et les coûts pour annuler les services offerts par Capital One et les remplacer par ceux d'une autre institution financière, puis ceux à encourir pour récupérer les sommes diverties et enfin, le montant correspondant à la perte de leur cotation aux fins d'obtenir du crédit auprès du marché financier résultant de cette intrusion.

[30] D'autre part, les demandeurs réclament des dommages moraux et non pécuniaires consistant en du stress, et autres troubles et inconvénients de cette nature, et qu'ils auraient subis et continueront de subir en raison de cet accès non autorisé à leurs renseignements personnels, et découlant, en substance, de leur crainte et de leur

anxiété générée par l'idée omniprésente de vivre encore longtemps avec le risque d'être éventuellement victimes d'une fraude.

[31] Enfin, les demandeurs réclament des défenderesses des dommages punitifs en vertu de l'article 49 de la *Charte des droits et libertés de la personne* [Charte]<sup>5</sup> et résultant de cette atteinte à leur droit à la protection de leur vie privée garanti par l'article 5 de la Charte, ainsi qu'en vertu des dispositions impératives de la *Loi sur la protection du consommateur*<sup>6</sup> [LPC] auxquelles les défenderesses auraient contrevenu, notamment en lien avec leur initiatives publicitaires et leurs représentations fausses ou trompeuses qu'elles auraient faites aux membres sur la qualité de la protection et de la sécurité entourant leurs renseignements personnels, et dont la violation permet, s'il est établi qu'il s'agit d'une pratique interdite, l'octroi de dommages punitifs en vertu de l'article 272 LPC.

[32] Le premier et le troisième critère prévus à l'article 575 C.p.c. sont satisfaits en l'espèce, soit l'existence de questions communes à débattre et qu'il n'existe pas d'autres moyens dans le C.p.c. eu égard à la composition du Groupe proposé que l'action collective pour faire valoir cette réclamation commune des demandeurs et des membres.

**II. Le critère prévu à l'article 575 al. 2 C.p.c. : les demandeurs ont-ils chacun une cause défendable à faire valoir à l'encontre des défenderesses?**

a) Le droit applicable au débat

[33] L'article 575 C.p.c. énonce que :

Le tribunal autorise l'exercice de l'action collective et attribue le statut de représentant au membre qu'il désigne s'il est d'avis que:

1° les demandes des membres soulèvent des questions de droit ou de fait identiques, similaires ou connexes;

2° les faits allégués paraissent justifier les conclusions recherchées;

3° la composition du groupe rend difficile ou peu pratique l'application des règles sur le mandat d'ester en justice pour le compte d'autrui ou sur la jonction d'instance;

4° le membre auquel il entend attribuer le statut de représentant est en mesure d'assurer une représentation adéquate des membres.

[34] Au stade de la demande d'autorisation, le fardeau des demandeurs est un de démonstration de la valeur du syllogisme juridique qu'ils proposent au soutien d'une

---

<sup>5</sup> RLRQ, c. C-12.

<sup>6</sup> RLRQ, c. P-40.1.

cause défendable à faire valoir par chacun d'eux contre les défenderesses<sup>7</sup>, et non d'établir, par prépondérance de preuve, qu'ils possèdent une cause suffisante d'action contre chacune de celles-ci.

[35] Dans l'arrêt qu'elle a rendu dans l'affaire *Desjardins Cabinet de services financiers inc. c. Asselin*<sup>8</sup>, la Cour suprême nous enseigne en effet que :

[81] En conclusion, non seulement les allégations sont présentes et suffisamment précises, mais elles sont également appuyées par la preuve au dossier. Rappelons qu'au Québec, la partie demanderesse n'est pas tenue, contrairement à ce qui est requis dans le reste du pays, de « démontrer[r] que sa demande repose sur un "fondement factuel suffisant" » (*Oratoire*, par. 58, citant *Infineon*, par. 128). En l'espèce, exiger une preuve documentaire déterminante du défaut d'information serait non seulement excessif à l'étape de l'autorisation, mais ce serait également imposer à M. Asselin un fardeau plus onéreux que celui auquel il devra faire face lors du procès sur le fond, puisque l'omission peut se prouver par tous les moyens, y compris le témoignage et l'inférence.

[36] À l'étape de l'autorisation qualifiée par la jurisprudence comme en étant une de filtrage seulement<sup>9</sup>, le Tribunal est uniquement appelé à déterminer si les quatre critères prévus à l'article 575 C.p.c. sont satisfaits.

[37] Selon les défenderesses, les demandeurs ne satisfont pas, en l'espèce, aux exigences découlant du deuxième et du quatrième critère énoncé à l'article 575 C.p.c., essentiellement pour les motifs suivants :

- A) la preuve offerte au stade de l'autorisation révèle que même si elle a réussi à obtenir accès aux renseignements personnels des membres recueillis par Capital One, puis hébergés dans un espace infonuagique public mis à leur disposition et géré par Amazon, Paige A. Thompson n'a pas, comme cela a été établi durant son procès criminel tenu aux États-Unis, communiqué ces renseignements à un tiers, ni fait un quelconque usage de ceux-ci, de sorte que ni les demandeurs, ni les membres putatifs n'ont subi un vol d'identité et n'en subiront vraisemblablement jamais un en rapport à cet incident;
- B) les défenderesses n'ont pas fait de représentations fausses ou trompeuses, ou posé des gestes entraînant une faute contractuelle ou extracontractuelle de leur part envers les demandeurs et les membres putatifs;
- C) Amazon soutient au surplus qu'il n'existe aucun lien de droit entre elle et les demandeurs et les membres putatifs, puisque ceux-ci sont identifiés

<sup>7</sup> *Saurette c. Astrazeneca Canada inc.*, 2019 QCCS 3323.

<sup>8</sup> 2020 CSC 30.

<sup>9</sup> *L'Oratoire Saint-Joseph du Mont-Royal c. J.J.*, 2019 CSC 35.



dans la désignation du Groupe proposé comme étant des clients de Capital One;

- D) même en tenant pour avérés les faits allégués par les demandeurs, ceux-ci n'allèguent, ni n'établissent, même par une preuve *prima facie*, aucun préjudice compensable au soutien de leur demande pour des dommages pécuniaires et non pécuniaires, faisant plutôt état de faits et de circonstances ne les concernant pas puisqu'allégués dans d'autres procédures pendantes devant d'autres juridictions au Canada et aux États-Unis, de sorte que les dommages qu'ils réclament sont purement hypothétiques;
- E) en ce qui concerne le demandeur Royer plus particulièrement, celui-ci, bien qu'ayant été avisé qu'il faisait partie des 6 000 000 résidents canadiens dont les renseignements personnels ont été rendus accessibles lors de cet incident de confidentialité survenu les 22 et 23 mars 2019, n'allègue pas, ni n'établit une utilisation illégale par quiconque de ses renseignements, ni qu'il ait subi un préjudice compensable, le tout n'étant que de simples hypothèses, conjectures ou de la pure spéculation;
- F) quant au demandeur Abou-Khadra, celui-ci ne fait pas partie de ce groupe de 6 000 000 résidents canadiens avisés de cette intrusion de sorte que ses renseignements personnels n'ont tout simplement pas été rendus accessibles lors de cet événement, alors que la fraude dont il allègue avoir été l'objet consiste plutôt en un usage non autorisé de sa carte de crédit, effectué par un tiers, du numéro de sa carte de crédit et de son code de sécurité (CCV), alors que de telles informations n'ont pas été rendues accessibles lors de l'incident survenu les 22 et 23 mars 2019 et que ce vol qu'il invoque découle plutôt, en ce qui le concerne, de la connaissance par un tiers de son numéro de carte de crédit et de son code secret, cela constituant une situation étrangère au débat soulevé en l'instance;
- G) les dommages pécuniaires et non pécuniaires réclamés par les demandeurs ne peuvent l'être en vertu du droit applicable au Québec, ces dommages n'étant pas non plus des inconvénients autres que ceux ordinairement vécus en de telles circonstances, ni graves ou sérieux, ni continus ou prolongés<sup>10</sup>;
- H) les dispositions législatives invoquées par les demandeurs à l'appui de leur réclamation pour des dommages punitifs ne trouvent pas application en l'espèce;

---

<sup>10</sup> *Mustapha c. Culligan*, 2008 CSC 27; *Zuckerman v. MGM Resorts International*, 2022 QCCS 2914.

- l) aucun des deux demandeurs ne possède par conséquent une cause défendable à faire valoir contre les défenderesses.

[38] Les défenderesses concluent que les deux demandeurs ne peuvent non plus, en raison de leur situation particulière à chacun d'eux et découlant des faits relatés ci-dessus, se voir attribuer le statut de représentant des membres putatifs leur permettant d'assurer une représentation adéquate de ceux-ci.

[39] À cet égard, les demandeurs soulignent que les faits qu'ils allèguent doivent être tenus pour avérés, sauf s'ils sont invraisemblables ou non plausibles<sup>11</sup>, et insistent sur le fait qu'il n'en va cependant pas de même des faits pouvant être allégués par les défenderesses<sup>12</sup>, comme l'a fait Capital One dans une déclaration sous serment de l'un de ses dirigeants, M. Jeffrey Behan<sup>13</sup>, qu'elle a produite à la suite d'une permission accordée en vertu de l'article 574 C.p.c. de présenter une preuve additionnelle<sup>14</sup>.

[40] Les défenderesses ne bénéficieraient donc pas de cette présomption quant à la valeur probante de la preuve qu'elles offrent.

[41] Les demandeurs ajoutent que même si les défenderesses peuvent avoir une défense sérieuse à faire valoir sur le fond de l'affaire, le Tribunal doit, à ce stade-ci des procédures, autoriser l'exercice de l'action collective projetée dès lors que la Demande d'autorisation propose un recours possiblement fondé<sup>15</sup>, en autant que celui-ci n'apparaisse pas frivole ou manifestement mal fondé à sa face même<sup>16</sup>.

[42] Selon les défenderesses, la difficulté, dans le cas présent, réside non pas dans la détermination par le Tribunal des faits qu'il doit retenir parmi ceux allégués par les demandeurs ou par les défenderesses parce que les parties proposeraient des versions contradictoires, ce qui n'est pas le cas ici, ni que cette trame factuelle présentée par les demandeurs soit contestée, puisqu'elle n'est pas réellement remise en cause par les défenderesses dans la présente affaire.

[43] La difficulté ici réside plutôt dans le fait, selon les défenderesses, que les allégations d'un préjudice subi, formulées dans la Demande, sont hypothétiques, spéculatives et purement théoriques, puisque la Demande fait défaut de révéler une véritable cause d'action défendable contre elles et que cet incident de confidentialité n'a eu finalement aucune conséquence pour les demandeurs, ni pour les membres putatifs.

---

<sup>11</sup> *Option Consommateurs c. Google*, 2022 QCCS 2308.

<sup>12</sup> *Durand c. Subway Franchise Systems of Canada*, 2020 QCCA 1647.

<sup>13</sup> Du 29 septembre 2021.

<sup>14</sup> *Benamor c. Air Canada*, 2020 QCCA 1597.

<sup>15</sup> *M.L. c. Guillot*, 2021 QCCA 1450.

<sup>16</sup> *Société québécoise de gestion collective des droits de reproduction (Copibec) c. Université Laval*, 2017 QCCA 199.

[44] Les défenderesses invitent donc le Tribunal à constater l'absence de faits précis allégués par les demandeurs quant aux conséquences de cet accès sur leurs renseignements personnels, et par conséquent, à conclure à l'inexistence d'une cause d'action défendable à faire valoir contre elles, faute d'un quelconque préjudice compensable.

[45] Toujours selon les défenderesses, les faits allégués par les demandeurs, auxquels s'ajoutent ceux révélés par la preuve additionnelle qu'elles ont été autorisées à présenter, révèlent, de façon claire et non équivoque, l'absence de syllogisme juridique pouvant supporter une cause d'action défendable en faveur du demandeur Abou-Khadra puisque les renseignements personnels de celui-ci n'ont pas été l'objet de cette intrusion car les achats non autorisés portés à sa carte de crédit sont sans lien avec cet événement cybernétique survenu au mois de mars 2019.

[46] Il convient, à cette étape de l'analyse, de rappeler que chaque demandeur doit établir l'existence d'une cause d'action défendable lui étant propre contre les défenderesses, indépendamment du fait que les membres puissent eux-mêmes posséder une telle cause d'action<sup>17</sup>.

[47] Les défenderesses ajoutent, en ce qui concerne le demandeur Royer, que celui-ci n'a subi aucun préjudice particulier même s'il fut avisé le 14 août 2019 de cette brèche informatique survenue les 22 et 23 mars 2019 dans le système de sécurité informationnelle mis en place par les défenderesses, parce que ses renseignements personnels n'ont pas été reproduits, ni distribués, ni utilisés, selon ce qu'il appert de la déposition de Paige A. Thompson

[48] Ce demandeur n'a donc eu aucun déboursé à effectuer, ni à encourir, et n'aura à supporter aucune dépense que ce soit, sauf de devoir vivre avec les inconvénients ordinaires en semblables circonstances<sup>18</sup>, étant compris que Capital One lui a offert, ainsi qu'aux membres putatifs, de supporter pendant deux années, les coûts de vérification et de surveillance de leurs comptes et relevés de cartes de crédit.

[49] Amazon ajoute enfin qu'il n'existe aucun lien de droit entre elle et les demandeurs, ni avec aucun des membres putatifs, puisqu'elle n'a transigé qu'avec Capital One dans cette affaire, comme en font foi les allégations de la Demande et les pièces invoquées au soutien de celle-ci, dont les formulaires d'adhésion émis par Capital One, ainsi que le contrat type qu'elle utilise présentement et sa politique de confidentialité qui y est stipulée.

[50] Toutefois, dans un extrait du site web de la défenderesse Amazon Web services Canada inc.<sup>19</sup>, celle-ci présente, en versions anglaise et française, les services qu'elle

---

<sup>17</sup> *Sofio c. Organisme canadien de réglementation du commerce des valeurs mobilières (OCRCVM)*, 2015 QCCA 1820.

<sup>18</sup> Préc. note 10.

<sup>19</sup> Pièce R-6.

offre au Canada aux consommateurs pour la conservation de leurs renseignements personnels.

[51] Si ce n'est pas en vertu du régime de la responsabilité contractuelle que Capital One puisse être jugée fautive, les demandeurs avancent que chacune des défenderesses a, de toute façon, engagé sa responsabilité extracontractuelle envers eux et les membres putatifs en vertu de l'article 1457 C.c.Q. qui prévoit que:

1457. Toute personne a le devoir de respecter les règles de conduite qui, suivant les circonstances, les usages ou la loi, s'imposent à elle, de manière à ne pas causer de préjudice à autrui.

Elle est, lorsqu'elle est douée de raison et qu'elle manque à ce devoir, responsable du préjudice qu'elle cause par cette faute à autrui et tenue de réparer ce préjudice, qu'il soit corporel, moral ou matériel.

Elle est aussi tenue, en certains cas, de réparer le préjudice causé à autrui par le fait ou la faute d'une autre personne ou par le fait des biens qu'elle a sous sa garde.

[52] Les demandeurs allèguent que les défenderesses ont également porté atteinte, en sus de leur droit à la protection de leur vie privée garanti par l'article 5 de la Charte, aux articles 35 à 37 C.c.Q., ainsi qu'aux dispositions pertinentes de la *Loi sur la protection des renseignements personnels et les documents électroniques*<sup>20</sup> [LPRPDE ou la loi canadienne], et à celles de la *Loi sur la protection des renseignements personnels dans le secteur privé*<sup>21</sup> [la loi québécoise].

[53] L'article 5 de la Charte stipule en effet que toute personne a droit au respect de sa vie privée et celle-ci s'applique aux défenderesses au Québec.

[54] *La loi (québécoise) sur la protection des renseignements personnels* définit ainsi l'étendue de son application :

1. La présente loi a pour objet d'établir, pour l'exercice des droits conférés par les articles 35 à 40 du Code civil en matière de protection des renseignements personnels, des règles particulières à l'égard des renseignements personnels sur autrui qu'une personne recueille, détient, utilise ou communique à des tiers à l'occasion de l'exploitation d'une entreprise au sens de l'article 1525 du Code civil.

Elle s'applique à ces renseignements quelle que soit la nature de leur support et quelle que soit la forme sous laquelle ils sont accessibles: écrite, graphique, sonore, visuelle, informatisée ou autre.

---

<sup>20</sup> L.C. 2000, c. 5.

<sup>21</sup> RLRQ, c. P-39.1.

Elle s'applique aussi aux renseignements personnels détenus par un ordre professionnel dans la mesure prévue par le Code des professions.

La présente loi ne s'applique pas à la collecte, la détention, l'utilisation ou la communication de matériel journalistique, historique ou généalogique à une fin d'information légitime du public.

Les sections II et III de la présente loi ne s'appliquent pas à un renseignement personnel qui a un caractère public en vertu de la Loi.

2. Est un renseignement personnel, tout renseignement qui concerne une personne physique et permet de l'identifier.

3. La présente loi ne s'applique pas:

1° à un organisme public au sens de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels.

2° aux renseignements qu'une personne autre qu'un organisme public détient, pour le compte de ce dernier.

3.1. Toute personne qui exploite une entreprise est responsable de la protection des renseignements personnels qu'elle détient.

Au sein de l'entreprise, la personne ayant la plus haute autorité veille à assurer le respect et la mise en œuvre de la présente loi. Elle exerce la fonction de responsable de la protection des renseignements personnels; elle peut déléguer cette fonction par écrit, en tout ou en partie, à toute personne.

Le titre et les coordonnées du responsable de la protection des renseignements personnels sont publiés sur le site Internet de l'entreprise ou, si elle n'a pas de site, rendus accessibles par tout autre moyen approprié.

[Le Tribunal souligne]

[55] Cette loi québécoise s'applique donc à toute personne exploitant une entreprise au Québec et qui détient des renseignements personnels sur une personne physique permettant de l'identifier.

[56] Les articles 3.5, 10, 28 et 29 de cette loi prévoient aussi des obligations particulières relatives à la protection, la sécurité, la prévention, et aussi à la diligence dont une entreprise assujettie doit faire preuve lorsque survient un incident de confidentialité :

3.5 Une personne qui exploite une entreprise et qui a des motifs de croire que s'est produit un incident de confidentialité impliquant un renseignement personnel qu'elle détient doit prendre les mesures raisonnables pour diminuer les risques

qu'un préjudice soit causé et éviter que de nouveaux incidents de même nature ne se produisent.

Si l'incident présente un risque qu'un préjudice sérieux soit causé, elle doit, avec diligence, aviser la Commission d'accès à l'information instituée par l'article 103 de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels. Elle doit également aviser toute personne dont un renseignement personnel est concerné par l'incident, à défaut de quoi la Commission peut lui ordonner de le faire. Elle peut également aviser toute personne ou tout organisme susceptible de diminuer ce risque, en ne lui communiquant que les renseignements personnels nécessaires à cette fin sans le consentement de la personne concernée. Dans ce dernier cas, le responsable de la protection des renseignements personnels doit enregistrer la communication.

10. Toute personne qui exploite une entreprise doit prendre les mesures de sécurité propres à assurer la protection des renseignements personnels collectés, utilisés, communiqués, conservés ou détruits et qui sont raisonnables compte tenu, notamment, de leur sensibilité, de la finalité de leur utilisation, de leur quantité, de leur répartition et de leur support.

28. Outre les droits prévus au premier alinéa de l'article 40 du Code civil, la personne concernée peut faire supprimer un renseignement personnel la concernant si sa collecte n'est pas autorisée par la loi.

29. Toute personne qui exploite une entreprise et détient des dossiers sur autrui doit prendre les mesures nécessaires pour assurer l'exercice par une personne concernée des droits prévus aux articles 37 à 40 du Code civil ainsi que des droits conférés par la présente loi. Elle doit notamment porter à la connaissance du public l'endroit où ces dossiers sont accessibles et les moyens d'y accéder.

[Le Tribunal souligne]

[57] Comme le révèlent les dispositions précitées de la loi québécoise, cette législation met en œuvre l'exercice des droits conférés par les articles 35 à 40 C.c.Q. en matière de protection des renseignements personnels, en énonçant des règles particulières à l'égard des renseignements personnels qu'une personne recueille sur autrui, détient, utilise ou communique à des tiers à l'occasion de l'exploitation d'une entreprise au sens de l'article 1525 C.c.Q.

[58] Il semble assez évident que ces dispositions législatives fournissent un cadre juridique de normes à respecter pour des entreprises comme celles exploitées par les défenderesses au Québec.

[59] Les articles 35 à 37 du C.c.Q. énoncent d'ailleurs que :

**35.** Toute personne a droit au respect de sa réputation et de sa vie privée.

Nulle atteinte ne peut être portée à la vie privée d'une personne sans que celle-ci y consente ou sans que la loi l'autorise.

**36.** Peuvent être notamment considérés comme des atteintes à la vie privée d'une personne les actes suivants:

1° Pénétrer chez elle ou y prendre quoi que ce soit;

2° Intercepter ou utiliser volontairement une communication privée;

3° Capter ou utiliser son image ou sa voix lorsqu'elle se trouve dans des lieux privés;

4° Surveiller sa vie privée par quelque moyen que ce soit;

5° Utiliser son nom, son image, sa ressemblance ou sa voix à toute autre fin que l'information légitime du public;

6° Utiliser sa correspondance, ses manuscrits ou ses autres documents personnels.

**37.** Toute personne qui constitue un dossier sur une autre personne doit avoir un intérêt sérieux et légitime à le faire. Elle ne peut recueillir que les renseignements pertinents à l'objet déclaré du dossier et elle ne peut, sans le consentement de l'intéressé ou l'autorisation de la loi, les communiquer à des tiers ou les utiliser à des fins incompatibles avec celles de sa constitution; elle ne peut non plus, dans la constitution ou l'utilisation du dossier, porter autrement atteinte à la vie privée de l'intéressé ni à sa réputation.

[60] Pour sa part, l'article 1525 C.c.Q. traite, comme nous le verrons plus loin, de la solidarité présumée entre les débiteurs d'une obligation contractée pour le service ou l'exploitation d'une entreprise.

[61] De son côté, la loi canadienne porte sur les renseignements personnels et les documents électroniques que gère une entreprise assujettie à cette loi.

[62] Elle pourrait s'appliquer en l'espèce, comme le prévoit son article 30, dans la mesure où l'Assemblée nationale du Québec n'a pas le pouvoir d'adopter une loi sur la cueillette, l'utilisation et la communication de renseignements personnels ou si une personne communique ces renseignements contre rémunération à l'extérieur du Québec, ce qui pourrait être le cas des défenderesses mais la preuve n'est pas suffisamment éloquente sur ce point :

**30.** La présente partie ne s'applique pas à une organisation à l'égard des renseignements personnels qu'elle recueille, utilise ou communique dans une province dont la législature a le pouvoir de régir la collecte, l'utilisation ou la

communication de tels renseignements, sauf si elle le fait dans le cadre d'une entreprise fédérale ou qu'elle communique ces renseignements pour contrepartie à l'extérieur de cette province.

[Le Tribunal souligne]

[63] Or, l'Assemblée nationale a le pouvoir de régir cette activité et l'a d'ailleurs exercé en adoptant la loi québécoise précitée.

[64] La loi canadienne peut également s'appliquer à Capital One et à Amazon si elles sont considérées comme des entreprises fédérales ou si elles ont communiqué, dans le cas présent, les renseignements personnels qu'elles détiennent, pour contrepartie, dans une autre province canadienne.

[65] La preuve offerte à ce stade-ci ne permet de statuer définitivement sur cette question, ce qui devra faire l'objet d'un débat devant le juge saisi du fond de cette affaire.

[66] La loi canadienne prévoit spécifiquement la possibilité de déposer une plainte auprès du Commissaire à la protection de la vie privée du Canada, et que la Cour fédérale du Canada est le tribunal compétent en cette matière pour entendre toute question qui a fait l'objet d'une plainte ou pour accorder une réparation, dont l'octroi de dommages et intérêts<sup>22</sup>.

[67] Les dispositions précitées de la Charte, de la loi québécoise sur les renseignements personnels et du *Code civil du Québec* sont donc celles qui sont assurément applicables aux défenderesses en l'espèce, à tout le moins à première vue, en ce qui a trait aux obligations statutaires pouvant leur incomber en matière de renseignements personnels dans la présente affaire, et possiblement celles de la loi canadienne, ce qui devra être démontré lors de l'instruction sur le mérite de cette affaire.

[68] Comme déjà mentionné, les demandeurs réclament aussi des dommages punitifs en vertu de l'article 49 de la *Charte des droits et libertés de la personne* et de l'article 272 LPC.

[69] En ce qui concerne l'application de l'article 272 LPC à la présente affaire, les demandeurs s'appuient sur les articles 34, 40 à 42, ainsi que sur les articles 215 à 219, 228, 253 et 271 de la LPC pour soutenir que les défenderesses ont exercé une pratique interdite en vertu de cette loi. Ces dispositions stipulent que :

**34.** La présente section s'applique au contrat de vente ou de louage de biens et au contrat de service.

[...]

---

<sup>22</sup> Articles 11 à 16 LPRPDE.



**40.** Un bien ou un service fourni doit être conforme à la description qui en est faite dans le contrat.

**41.** Un bien ou un service fourni doit être conforme à une déclaration ou à un message publicitaire faits à son sujet par le commerçant ou le fabricant. Une déclaration ou un message publicitaire lie ce commerçant ou ce fabricant.

**42.** Une déclaration écrite ou verbale faite par le représentant d'un commerçant ou d'un fabricant à propos d'un bien ou d'un service lie ce commerçant ou ce fabricant.

**43.** Une garantie relative à un bien ou à un service, mentionnée dans une déclaration ou un message publicitaire d'un commerçant ou d'un fabricant, lie ce commerçant ou ce fabricant. Il en est de même d'une garantie écrite du commerçant ou du fabricant non reproduite dans le contrat.

[...]

**215.** Constitue une pratique interdite aux fins du présent titre une pratique visée par les articles 219 à 251.2 ou, lorsqu'il s'agit de la vente, de la location ou de la construction d'un immeuble, une pratique visée aux articles 219 à 222, 224 à 230, 232, 235, 236 et 238 à 243.

**216.** Aux fins du présent titre, une représentation comprend une affirmation, un comportement ou une omission.

**217.** La commission d'une pratique interdite n'est pas subordonnée à la conclusion d'un contrat.

**218.** Pour déterminer si une représentation constitue une pratique interdite, il faut tenir compte de l'impression générale qu'elle donne et, s'il y a lieu, du sens littéral des termes qui y sont employés.

**219.** Aucun commerçant, fabricant ou publicitaire ne peut, par quelque moyen que ce soit, faire une représentation fausse ou trompeuse à un consommateur.

[...]

**228.** Aucun commerçant, fabricant ou publicitaire ne peut, dans une représentation qu'il fait à un consommateur, passer sous silence un fait important.

[...]

**253.** Lorsqu'un commerçant, un fabricant ou un publicitaire se livre en cas de vente, de location ou de construction d'un immeuble à une pratique interdite ou, dans les autres cas, à une pratique interdite visée aux paragraphes a et b de l'article 220, a, b, c, d, e et g de l'article 221, d, e et f de l'article 222, c de l'article 224, a et b de l'article 225 et aux articles 227, 228, 229, 237 et 239, il y a présomption que, si le

consommateur avait eu connaissance de cette pratique, il n'aurait pas contracté ou n'aurait pas donné un prix si élevé.

[...]

**271.** Si l'une des règles de formation prévues par les articles 25 à 28 n'a pas été respectée, ou si un contrat ne respecte pas une exigence de forme prescrite par la présente loi ou un règlement, le consommateur peut demander la nullité du contrat.

Dans le cas d'un contrat de crédit, lorsqu'une modalité de paiement ou encore le calcul ou une indication des frais de crédit ou du taux de crédit n'est pas conforme à la présente loi ou à un règlement, le consommateur peut demander, à son choix, soit la nullité du contrat, soit la suppression des frais de crédit et la restitution de la partie des frais de crédit déjà payée.

Le tribunal accueille la demande du consommateur sauf si le commerçant démontre que le consommateur n'a subi aucun préjudice du fait qu'une des règles ou des exigences susmentionnées n'a pas été respectée.

**272.** Si le commerçant ou le fabricant manque à une obligation que lui impose la présente loi, un règlement ou un engagement volontaire souscrit en vertu de l'article 314 ou dont l'application a été étendue par un décret pris en vertu de l'article 315.1, le consommateur, sous réserve des autres recours prévus par la présente loi, peut demander, selon le cas:

- a) l'exécution de l'obligation;
- b) l'autorisation de la faire exécuter aux frais du commerçant ou du fabricant;
- c) la réduction de son obligation;
- d) la résiliation du contrat;
- e) la résolution du contrat; ou
- f) la nullité du contrat,

sans préjudice de sa demande en dommages-intérêts dans tous les cas. Il peut également demander des dommages-intérêts punitifs.

[Le Tribunal souligne]

[70] En ce qui concerne l'application de l'article 272 LPC, les demandeurs doivent d'abord satisfaire aux quatre critères énoncés par la Cour suprême dans l'affaire *Richard c. Time inc.*<sup>23</sup> qui nous propose un cadre d'analyse afin de déterminer l'application de la présomption de préjudice prévue à la LPC au cas de pratique interdite:

---

<sup>23</sup> 2012 CSC 8.

**124.** L'application de la présomption absolue de préjudice présuppose qu'un lien rationnel existe entre la pratique interdite et la relation contractuelle régie par la loi. Il importe donc de préciser les conditions d'application de cette présomption dans le contexte de la commission d'une pratique interdite. À notre avis, le consommateur qui souhaite bénéficier de cette présomption doit prouver les éléments suivants : (1) la violation par le commerçant ou le fabricant d'une des obligations imposées par le titre II de la loi; (2) la prise de connaissance de la représentation constituant une pratique interdite par le consommateur; (3) la formation, la modification ou l'exécution d'un contrat de consommation subséquente à cette prise de connaissance, et (4) une proximité suffisante entre le contenu de la représentation et le bien ou le service visé par le contrat. Selon ce dernier critère, la pratique interdite doit être susceptible d'influer sur le comportement adopté par le consommateur relativement à la formation, à la modification ou à l'exécution du contrat de consommation. Lorsque ces quatre éléments sont établis, les tribunaux peuvent conclure que la pratique interdite est réputée avoir eu un effet dolosif sur le consommateur. Dans un tel cas, le contrat formé, modifié ou exécuté constitue, en soi, un préjudice subi par le consommateur. L'application de cette présomption lui permet ainsi de demander, selon les mêmes modalités que celles décrites ci-dessus, l'une des mesures de réparation contractuelles prévues à l'art. 272 *L.p.c.*

[Le Tribunal souligne]

[71] Toutefois, dès qu'une attitude négligente et insouciante d'une personne est établie à l'égard d'autrui, du public ou d'un consommateur, une telle conduite peut être, pour l'essentiel, assimilée à une atteinte ou à une contravention intentionnelle<sup>24</sup>, ou encore lorsque cette personne agit en pleine connaissance des conséquences immédiates et naturelles, ou à tout le moins extrêmement probables, découlant de sa conduite<sup>25</sup>.

[72] Selon les demandeurs, il y a eu en l'espèce une telle négligence par les défenderesses envers les demandeurs et les membres putatifs, puisqu'elles ont fait des représentations sur la fiabilité de leur système de sécurité informationnelle, et ce, alors que les défenderesses étaient pleinement conscientes de la vulnérabilité de ce même système d'hébergement et de conservation des renseignements personnels des membres depuis au moins l'année 2015.

[73] Les demandeurs ajoutent que par leurs représentations publiques et par leur publicité en général, tant sur leur formulaire d'adhésion que sur leur site web respectif, notamment quant à Capital One et sa politique de confidentialité dont nous discuterons plus loin, et Amazon, dans une mesure peut-être différente dans ce dernier cas, les défenderesses ont fait des représentations fausses ou trompeuses aux demandeurs et

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

<sup>25</sup> *Levy v. Nissan Canada inc.*, 2021 QCCA 682.

aux membres, lesquelles constitueraient des pratiques interdites en vertu des articles 215 et suivants précités de la LPC.

[74] Les demandeurs concluent qu'en vertu des articles 253 et 271 de cette loi, les membres bénéficient à la fois de cette présomption de l'existence d'une pratique interdite ayant entraîné leur adhésion auprès de Capital One, ainsi que de cette présomption qu'un préjudice a été subi par les membres sans qu'il ne leur soit nécessaire d'en faire la preuve, de sorte que les défenderesses sont tenues à des dommages punitifs en vertu de l'article 272 LPC, les demandeurs ne devant prouver uniquement que la présence de représentations fausses ou trompeuses, sans qu'il ne leur soit nécessaire de démontrer un préjudice.

[75] Selon les défenderesses, ces dispositions ne sont pas applicables au contrat de crédit pouvant lier les demandeurs et les membres aux défenderesses du groupe Capital One, puisque les articles 40 à 42 de la LPC se trouvent dans une section particulière de cette loi consacrée uniquement au contrat de vente ou de louage d'un bien ou de service, et non au contrat de crédit.

[76] Elles réfèrent tout particulièrement aux articles 36 et suivants de la LPC, sous le chapitre III de celle-ci relatif au contrat de vente ou de louage de biens et au contrat de service.

[77] Le Tribunal observe dans un premier temps que le Titre 1 de la LPC s'étend à tous les contrats portant sur un bien ou un service, et que son chapitre I prévoit des dispositions applicables généralement à tous ces contrats.

[78] Au chapitre III, toujours sous ce même Titre 1, la LPC traite généralement des contrats se rapportant à la vente ou au louage d'un bien ou de service et prévoit, sous sa section I, des obligations générales applicables à ces contrats et nécessairement additionnelles à celles prévues au chapitre I discuté ci-dessus.

[79] Le chapitre III se consacre ensuite, sous différentes sections, dont la section III portant sur les contrats de crédit, aux obligations spécifiques, et à nouveau additionnelles, devant être appliquées à différents types de contrats de consommation, selon la nature du contrat en particulier dont il est question dans chacune de ces sections, dont les contrats de crédit, lesquels contrats demeurent néanmoins assujettis aux obligations générales applicables aux contrats de vente et de louage d'un bien et de service prévues au chapitre I.

[80] En l'espèce, le contrat de consommation liant les membres putatifs et Capital One est non seulement, selon les termes de la LPC, régi par les dispositions particulières relatives aux contrats de crédit prévues à cette loi, car le contrat de consommation invoqué en l'espèce est un contrat de service visant ici divers services financiers incluant le crédit, mais celui-ci demeure également régi par les dispositions générales prévues au chapitre I, titre 1 de la LPC, dont les articles 40 et suivants de cette loi.

[81] De plus, rien dans les autorités citées par les défenderesses n'indiquent que les dispositions générales prévues aux articles 35 et suivants de la LPC relatives aux contrats de vente et de louage de biens et de service, ne s'appliquent pas à ce contrat de service particulier afférent à l'émission par Capital One d'une carte de crédit en faveur des membres.

[82] Par conséquent, le contrat de consommation conclu entre les demandeurs et les membres putatifs d'une part, et Capital One d'autre part, pourrait être régi par les dispositions de la LPC.

b) Le demandeur Abou-Khadra

[83] Le demandeur Abou-Khadra ne formule aucune allégation, et n'offre aucune preuve permettant d'établir, même de façon *prima facie*, que ses renseignements personnels ont été la cible d'un accès non autorisé lors de cet incident de confidentialité survenu au mois de mars 2019, étant établi par ailleurs qu'il ne fait pas partie de ces 6 000 000 de résidents canadiens qui ont été avisés par les défenderesses du groupe Capital One de cet événement, auxquels se sont subséquemment ajoutés 51 000 autres résidents canadiens.

[84] Les faits qu'il allègue et ceux relatés par Capital One dans le cadre de cette preuve additionnelle qu'elle a été autorisée à présenter au moyen de cette déclaration sous serment précitée de M. Jeffrey Behan du 29 septembre 2021, révèlent clairement et sans aucune ambiguïté, que ces deux transactions non autorisées portées au relevé de compte de la carte de crédit de ce demandeur, pour des montants de 267 \$ et de 2,55\$<sup>26</sup>, sont sans relation avec l'incident de confidentialité survenu les 22 et 23 mars 2019.

[85] Selon cette déclaration de M. Behan, les deux transactions portées au relevé de la carte de crédit du demandeur Abou-Khadra<sup>27</sup> résultent de l'utilisation du numéro de sa carte de crédit, donné par téléphone au commerçant concerné, en l'occurrence, la société Power Keto, ainsi que du numéro de son code secret se trouvant à l'endos de sa carte de crédit et qui aurait également été divulgué par téléphone à ce commerçant.

[86] Or, toujours selon la déclaration de M. Behan, aucun numéro de compte de banque, ni de carte de crédit, ni aucun numéro de code secret, tout comme aucun numéro d'assurance sociale, n'a été l'objet de ce bris de confidentialité survenu les 22 et 23 mars 2019.

[87] Soulignons enfin que les faits allégués à cette déclaration sous serment de M. Behan fournie par Capital One ne sont pas contredits.

[88] Fort de cette preuve, le Tribunal ne peut appliquer en l'espèce, comme le proposent les demandeurs, cette notion de contemporanéité ou de *timing* existant entre

---

<sup>26</sup> Pièce P-29.

<sup>27</sup> Pièce R-29.

les événements survenus les 22 et 23 mars 2019 et les transactions non autorisées qui furent portées au compte d'Abou-Khadra, puisqu'une preuve spécifique est présentée dans le présent cas pour écarter cette possibilité ou cette hypothèse pouvant prendre la forme d'une sorte de présomption et découlant simplement de la proximité de ces deux événements dans le temps.

[89] Au surplus, dans les conclusions de l'action collective qu'ils proposent quant au Groupe et aux avis à être donnés aux membres, les demandeurs ont, de toute façon, eux-mêmes exclu les personnes se trouvant dans la même situation que celle du demandeur Abou-Khadra, puisque ces personnes ne peuvent être identifiées adéquatement et que le Groupe désigné des membres identifie ceux dont les données ont été compromises lors de l'incident survenu au mois de mars 2019, ce qui exclut le demandeur Abou-Khadra.

[90] L'action collective projetée ne sera donc pas autorisée en ce qui concerne ce demandeur.

c) Capital One

*La faute*

[91] Afin de supporter le syllogisme juridique qu'ils invoquent contre Capital One, les demandeurs s'appuient sur le formulaire d'application publié par cette dernière en 2019, et qu'ils auraient chacun utilisé plusieurs années auparavant lors de leur adhésion respective, pour l'une ou l'autre de ces six catégories de cartes de crédit offertes<sup>28</sup> par cette institution financière.

[92] Ce formulaire requiert divers renseignements personnels des personnes produisant cette demande d'adhésion<sup>29</sup>, dont leur numéro d'assurance sociale, en vue d'obtenir une carte de crédit Costco dont Capital One est l'émettrice.

[93] Les demandeurs réfèrent ensuite aux documents publiés sur le site web de Capital One<sup>30</sup> et dans lesquels sont énoncés les termes et conditions de la politique de confidentialité de cette dernière, dans sa version datant de 2020, et des textes décrivant les mesures de sécurité mises en place par Capital One.

[94] Les demandeurs s'appuient sur ces documents pour établir non seulement la faute contractuelle de Capital One envers les membres putatifs, mais également pour soutenir l'existence de représentations fausses ou trompeuses de sa part, notamment à partir de 2015, sur les mesures de protection et de sécurité mises en place par celle-ci pour protéger le caractère privé et confidentiel de leurs renseignements personnels.

---

<sup>28</sup> Pièce R-7.

<sup>29</sup> Pièce R-8.

<sup>30</sup> Pièces R-11 et R-15.

[95] Voici un extrait de la politique de confidentialité de Capital One<sup>31</sup> :

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, if 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.

- 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?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.

[Le Tribunal souligne]

[96] Les extraits précités de cette politique de confidentialité et ceux plus bas révèlent que les parties conviennent d'incorporer à leur contrat la définition des termes « Renseignements confidentiels » qui se retrouve à la loi canadienne (PIPEDA), ce qui ne rend pas pour autant, cela étant dit, cette loi applicable aux parties dans le cas présent<sup>32</sup>, comme déjà discuté ci-dessus, de sorte que seule cette définition est incorporée au contrat liant les parties.

[97] Ces extraits stipulent que Capital One s'engage à utiliser ces renseignements, entre autres, dans un but de prévention de la fraude et aux fins prévues notamment par la loi et les normes de l'industrie applicables.

[98] Les documents précités devaient, selon les demandeurs, se lire sensiblement de la même façon lors de leur adhésion, et soulignent que les versions pertinentes pourront être obtenues en temps utile avant l'instruction portant sur le mérite de l'affaire.

---

<sup>31</sup> Pièce R-15.

<sup>32</sup> *Id.*

[99] Les autres documents sont de la nature d'avis ou de communiqués retrouvés sur les sites web des défenderesses<sup>33</sup>.

[100] Au soutien de leur plan d'argumentation du 19 décembre 2022, les demandeurs réfèrent à un document plus complet intitulé *Customer Agreement*, et qui énonce les termes et conditions du contrat de consommation conclu entre les membres et Capital One<sup>34</sup>.

[101] Ils produisent ce contrat, sous objection toutefois<sup>35</sup>, afin d'exposer le contenu intégral de ce document, dont tous les termes et conditions de la politique de confidentialité de Capital One à l'égard des renseignements personnels obtenus de ses clients.

[102] Le Tribunal en reproduit ici quelques extraits<sup>36</sup> :

#### **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:

---

<sup>33</sup> Pièces R-6 et R-58.

<sup>34</sup> Pièce R-93, version de 2022.

<sup>35</sup> Les défenderesses soutiennent que les documents R-8, R-15, R-16 et R-93 sont postérieurs à 2015 et ajoutent quant à cette dernière pièce, ainsi que pour les pièces R-94 et R-95, que cette façon de procéder des demandeurs est irrégulière et illégale en ce que les documents qu'ils invoquent, doivent être allégués et invoqués comme pièces au soutien de la Demande et non de leur plan d'argumentation, ce à quoi il fut remédié à l'audience par une demande de modification verbale de la Demande.

<sup>36</sup> Pièce R-93.



- 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 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.

[Le Tribunal souligne]

[103] Certains documents sont mentionnés pour la première fois dans le plan d'argumentation des demandeurs déposé en vue de l'instruction sur la Demande<sup>37</sup>, malgré les quatre modifications apportées à celle-ci.

---

<sup>37</sup> Pièces P-93 à P-95.

[104] Les demandeurs justifient leur geste par la non-disponibilité de ces documents avant l'instruction, et qu'ils ont finalement, et sans doute, obtenus ceux-ci à la suite d'une recherche dans les deux autres dossiers judiciaires similaires précités et toujours pendants au Canada<sup>38</sup>.

[105] À cet égard, le Tribunal ne peut faire obstacle aux prétentions des demandeurs du seul fait qu'ils s'appuient sur des documents postérieurs de quelques années à l'incident survenu en 2019 et leur en faire grief, puisque qu'il peut à ce stade-ci, simplement s'en remettre aux allégations des demandeurs, qu'ils devront éventuellement prouver, voulant que ces documents aient stipulé de tels engagements lors de l'adhésion des demandeurs plusieurs années auparavant, vraisemblablement en 2005.

[106] Cette difficulté à obtenir l'ensemble des données et documents pertinents est inhérente à toute demande au stade de l'autorisation, et elle pourra être surmontée au stade l'instruction de cette affaire, comme le rappelait le juge Kasirer dans l'affaire *Asselin*<sup>39</sup>, après la tenue des interrogatoires préalables et la mise en œuvre des autres moyens de preuve précédant l'instruction.

[107] Les demandeurs reprochent à Capital One d'avoir conservé pendant de nombreuses années des renseignements personnels devenus objectivement inutiles avec le passage du temps et d'autres sans justification, puisqu'ils furent obtenus dans ce dernier cas, de personnes s'étant vu refuser le crédit sollicité.

[108] Selon les demandeurs, ces renseignements qui sont encore privés et confidentiels à ce jour, ont pu néanmoins continuer à servir, même s'ils sont devenus inutiles, les objectifs commerciaux et les projets lucratifs fomentés par les défenderesses.

[109] La période de conservation de ces renseignements personnels s'échelonne, dans certains cas, jusqu'à 14 ans, soit depuis l'adhésion des demandeurs à la date de l'incident de confidentialité, et selon les informations obtenues par les demandeurs, le furent uniquement à des fins de permettre le développement de logiciels d'intelligence artificielle par Amazon, notamment pour sonder les habitudes de crédit et de consommation des membres pour leur offrir de nouveaux produits et services.

[110] Les demandeurs expliquent dans leur Demande et plaident également à l'audience, en s'appuyant sur des articles d'observateurs du milieu, pour certains publiés sur le web ou par des revues spécialisées<sup>40</sup>, que Capital One a procédé au mois d'octobre 2015 à une migration des renseignements personnels qu'elle détient alors, puisque devenue alors inévitable vu la trop grande quantité de données en cause, vers

---

<sup>38</sup> Voir les extraits reproduits dans les deux jugements précités des juges Perell et Iver., préc., notes 3 et 4.

<sup>39</sup> Préc., note 9.

<sup>40</sup> Pièces R-11 à R-13.

les serveurs d'Amazon, publics et moins étanches, donc moins sécuritaires que ceux de Capital One.

[111] L'accès non autorisé des 22 et 23 mars 2019 serait le fait d'une ancienne employée de la défenderesse Amazon web services inc. certes, mais selon Amazon, cette intrusion a été causée par une mauvaise configuration par Capital One d'un système de protection requis et devant être installé lors de cette migration massive des renseignements personnels détenus par Capital One<sup>41</sup>, et que cette déficience aurait été exacerbée par des autorisations d'accès trop larges accordées par Capital One.

[112] Les demandeurs indiquent que la cause de cet incident de confidentialité réside plutôt dans l'architecture déficiente choisie par Capital One, mais dont la mise en place ne fut rendue possible que par le concours d'Amazon, de sorte que c'est par ce choix commun de ce procédé par Capital One et Amazon, appelé *Cloud Custodian*, qui devait prémunir leur système de toute vulnérabilité, que ce malheureux incident de confidentialité a pu survenir, qu'il n'a pu être prévu, ni être empêché<sup>42</sup>.

[113] Les allégations de la Demande et certaines pièces<sup>43</sup> font d'ailleurs état d'une forme d'association entre Capital One et Amazon lors de la mise en place de cet environnement de conservation et d'hébergement des renseignements personnels et du traitement de ceux-ci par différents logiciels qu'elles ont développés, essentiellement par Amazon, afin d'optimiser leurs offres de produits et de services, puis pour la vente de ceux-ci.

[114] De possibles recours peuvent ainsi être éventuellement envisagés entre Capital One et Amazon, possiblement en cette instance ou dans une autre, mais ces recours sont de peu d'importance à ce stade-ci de notre réflexion, car il s'agit que la Demande révèle cette possibilité qu'une faute contractuelle ait pu être commise par Capital One à qui les membres putatifs ont confié leurs renseignements personnels, pour que les demandeurs franchissent un premier pas dans le cadre de cette étape de filtrage.

[115] Ce service infonuagique public et géré par Amazon est décrit comme se composant d'imposants bassins ou lacs (« lakes ») de données, et serait, au sein de l'ensemble de l'industrie, réputé comme étant moins fiable que d'autres systèmes semblables, faisant en sorte qu'il est redouté et boudé par différentes institutions financières, et même par d'autres grandes entreprises technologiques comme Google et Microsoft, puisque représentant un risque plus élevé de brèches dans les systèmes de sécurité informationnelle.

[116] Cette importante vulnérabilité aurait déjà été mise en lumière auparavant, entre autres, par des incidents déjà survenus aux États-Unis entre 2016 et 2019, et ayant donné lieu à des pénalités imposées aux défenderesses du groupe Capital One par

---

<sup>41</sup> Pièces R-39 a) et b).

<sup>42</sup> Par. 10.58 de la Demande et pièce R-14.

<sup>43</sup> Pièces R-12.

l'organisme de surveillance américain compétent en cette matière<sup>44</sup> en relation avec les procédés internes d'évaluation des risques mis en place par Capital One<sup>45</sup>, ce que souligneraient à grands traits plusieurs demandes de certification d'actions collectives déposées aux États-Unis et qui furent éventuellement réunies devant une même juridiction américaine<sup>46</sup>.

[117] Les demandeurs relatent également qu'à la suite de l'accès non autorisé survenu les 22 et 23 mars 2019, la vulnérabilité du système d'Amazon à l'égard de telles intrusions [appelées SSRF] fut signalée à celle-ci le 14 avril 2019<sup>47</sup> par l'un de ses employés auprès de son supérieur<sup>48</sup>, mais que Capital One a, malgré cela, tardé à agir, n'ayant découvert cette intrusion que le 17 juillet 2019 suite à une communication par un tiers, et alors que la masse astronomique d'informations compromises, donc rendues accessibles, comprenaient notamment des noms, adresses, numéros de téléphone, dates de naissance, numéros d'assurance sociale et autres données sur le dossier de crédit des millions d'individus concernés.

[118] Les demandeurs ajoutent que Capital One a également été négligente par la suite, faute d'avoir diligemment informé ses clients de cette intrusion, et pour finalement ne leur avoir offert qu'une solution bien imparfaite et insuffisante, consistant en des services gratuits, pour une durée de deux années seulement, offerts par des firmes externes comme les sociétés Équifax et TransUnion, de surveillance des entrées inscrites à leurs relevés de comptes pour y déceler, le cas échéant, toute irrégularité pouvant résulter d'une appropriation illégale de données privées et confidentielles.

[119] À ce sujet, les demandeurs soutiennent que plusieurs membres ont fait valoir leur mécontentement à l'égard de cette offre de surveillance gratuite de leurs comptes pour une durée de deux ans, arguant qu'ils peuvent néanmoins être victimes de fraude, d'un vol de données et d'identité, sans que cela ne puisse être décelé, et alors que le risque d'un tel geste illégal s'étend sur un beaucoup plus grand nombre d'années qu'une période de deux ans, de sorte qu'il en coûtera vraisemblablement aux membres, des frais de surveillance s'élevant à quelques centaines de dollars annuellement.

[120] Les demandeurs soulignent enfin que les défenderesses ont quand même maintenu ce système déficient de protection et de sécurité par la suite<sup>49</sup>, bien que ce soit la Banque Canadienne Impériale de Commerce qui désormais émet les cartes de crédit de la bannière Costco, et ce, depuis le mois d'avril 2022.

---

<sup>44</sup> *US Office of the Comptroller of the Currency.*

<sup>45</sup> Par. 10.74 et suivants de la Demande

<sup>46</sup> Ayant fait l'objet d'une transaction le 31 janvier 2022 avant la présentation de la demande de certification prévue le lendemain.

<sup>47</sup> Pièce R-18.

<sup>48</sup> Pièce R-89.

<sup>49</sup> Par. 10.59 de la Demande.

[121] En raison de ce qui précède, le Tribunal est d'avis que les allégations de la Demande révèlent que Capital One a pu commettre une faute de nature contractuelle envers le demandeur Royer et les membres putatifs à l'origine de cette intrusion non autorisée vers leurs renseignements personnels au mois de mars 2019.

[122] Les documents invoqués par les demandeurs<sup>50</sup> contiennent en effet des énoncés suffisants pour soutenir l'existence d'une faute contractuelle de la part de Capital One envers Royer et les membres putatifs, notamment par voie de référence aux normes législatives applicables et de l'industrie, particulièrement en ce qui a trait aux risques associés à cette migration des données en 2015, par la mise en place de mesures de protection insuffisantes et inefficaces malgré des indications et des alertes provenant de différents acteurs de l'industrie et des autorités règlementaires compétentes, mais qui ont été ignorées par Capital One.

[123] Cette faute potentielle de Capital One peut aussi découler de la conservation de données pour certaines en rapport à des membres dont le crédit fut refusé, et pour un grand nombre, sur une période déraisonnablement longue.

[124] Cette faute découlerait ainsi d'un possible manquement de Capital One aux engagements résultant de son formulaire d'adhésion rempli par les membres putatifs<sup>51</sup> et du contrat de consommation en résultant conclu entre les parties, incorporant cette politique de confidentialité relative aux renseignements personnels obtenus de ses clients, lesquels documents réfèrent au surplus à la législation et la réglementation applicables, dont les dispositions récitées de la loi québécoise sur la protection des renseignements personnels, celles du C.c.Q. et possiblement celles de la loi canadienne.

[125] Capital One n'aurait donc pas, malgré les termes du contrat conclu avec les membres, les dispositions législatives lui étant applicables et les normes reconnues en matière de sécurité informationnelle dans l'industrie, protégé adéquatement les renseignements personnels de ses clients et leur droit à la protection de leur vie privée, ni déployé tous les moyens requis, ni fait preuve de la prudence et de la diligence élémentaires à cette fin pouvant être normalement requises et auxquels pouvaient s'attendre les membres putatifs, contrevenant ainsi à ses obligations contractuelles, incluant les obligations statutaires précitées et lui être applicables, et ce, lors de cette intrusion non autorisée survenue en mars 2019, puis ensuite de ne pas avoir prévenu un tel incident de confidentialité devenu possible sinon probable suite à cette migration massive des renseignements personnels de ses clients en 2015 vers le service infonuagique offert par Amazon, ni d'avoir remédié aux déficiences de son système par la suite.

---

<sup>50</sup> *Id.*

<sup>51</sup> Pièces R-8, R-15, R-58 et R-93.

*Les représentations fausses ou trompeuses*

[126] Les demandeurs reprochent également à Capital One d'avoir représenté faussement à ses clients, depuis de nombreuses années, la valeur et la fiabilité de son système de protection et de sécurité des renseignements personnels obtenus de leurs clients, incitant ces derniers à leur confier leurs renseignements personnels.

[127] Les demandeurs s'appuient sur les mêmes documents que ceux précités pour établir la faute de Capital One envers les membres putatifs, mais cette fois-ci pour plaider l'existence de représentations fausses ou trompeuses de sa part, notamment en 2015, sur les mesures de protection et de sécurité apparemment mises en place pour protéger le caractère privé et confidentiel de leurs renseignements personnels<sup>52</sup>.

[128] Les demandeurs invoquent donc à nouveau le contenu de ces documents contractuels quant à Capital One, ainsi que les extraits de son site web, pour faire état de telles représentations fausses ou trompeuses, également en ce qui concerne Amazon comme nous le verrons plus loin<sup>53</sup>.

[129] En premier lieu, la demande est silencieuse sur le fait que les demandeurs aient pu prendre ou non connaissance du contenu de tous ces documents avant de remplir leur demande d'adhésion auprès de Capital One et de contracter avec cette dernière.

[130] De plus, rien dans les allégations de la Demande ne démontre qu'une information donnée aux demandeurs et aux membres par Capital One, ou publiée par celle-ci, se soit subséquemment avérée fausse ou trompeuse à un moment ou un autre notamment entre 2015 et 2019.

[131] L'incident de confidentialité survenu en mars 2019 peut certes être invoqué pour démontrer l'existence d'une faute, mais il n'en demeure pas moins qu'aucune des allégations de la Demande n'identifie spécifiquement une représentation particulière, écrite ou orale, faite auparavant par Capital One, qui serait fausse ou trompeuse à cet égard, et qu'elle le fut dans le but d'amener les membres à contracter avec elle.

[132] Ainsi, même si un contrat de consommation a pu être conclu entre les demandeurs et les membres d'une part, et Capital One d'autre part, rendant ainsi la LPC applicable à cette dernière, le Tribunal estime que la preuve qui lui a été présentée et les allégations de la Demande, sont insuffisantes, trop vagues, générales et imprécises pour soutenir que Capital One ait pu faire aux membres de telles représentations fausses ou trompeuses, au sens donné à cette expression dans la LPC, pour constituer une pratique interdite selon la LPC, et permettant aux membres de réclamer de celle-ci des dommages punitifs en vertu de l'article 272 LPC.

---

<sup>52</sup> Pièces R-15 et R-16.

<sup>53</sup> Pièces R-6, R-11 et R-15.

d) Amazon

*La faute*

[133] Amazon plaide qu'elle n'a aucun lien de droit avec les membres putatifs, mais uniquement avec Capital One, et que ce lien contractuel consiste seulement à permettre à Capital One d'héberger sur son espace infonuagique les renseignements personnels obtenus des clients de cette dernière et qui résident au Québec.

[134] Selon Amazon, non seulement elle n'a pris aucun engagement, ni contracté d'obligation contractuelle envers les membres, mais c'est au surplus à Capital One que les membres ont confié leurs renseignements personnels, de sorte que les lois provinciale ou canadienne ne peuvent être applicables à Amazon.

[135] Amazon ajoute qu'elle n'a fait aucune représentation, ni adressé quelque publicité que ce soit aux demandeurs, ni aux membres putatifs, et elle plaide que les informations se trouvant sur son site web et s'adressant aux canadiens, ni visent en fait que les entreprises et non les personnes physiques<sup>54</sup>.

[136] Or, le site web d'Amazon ne fait pas cette distinction, son contenu s'adressant à tout consommateur canadien.

[137] Malgré cela, Amazon conclut donc qu'il ne peut lui être davantage reproché d'avoir commis une faute extracontractuelle envers les demandeurs et les membres putatifs.

[138] Amazon est possiblement à l'origine de cet incident de confidentialité, ce qui peut s'inférer du fait que l'auteur de cette intrusion est l'une de ses anciennes employées, et qui a sans doute pu, pendant la durée de son emploi, accéder à toutes procédures de contrôle, de vérification et de protection des données et également à tous ces renseignements personnels censés être adéquatement protégés.

[139] D'entrée de jeu, Amazon a possiblement commis une ou plusieurs fautes, engageant vraisemblablement sa responsabilité contractuelle envers Capital One dans le cadre d'un éventuel recours en garantie, ce qui n'est pas l'objet ici de notre analyse.

[140] Il n'y a pas ou très peu à douter d'ailleurs qu'un litige naisse éventuellement entre Amazon et Capital One, si ce n'est déjà le cas, dans l'éventualité où une action collective est éventuellement autorisée contre Capital One.

[141] Le Tribunal observe d'ailleurs déjà que dans les pièces invoquées par les demandeurs, Capital One et Amazon ont déjà, plus d'une fois, attribué à l'autre la responsabilité ultime de cet accès non autorisé.

---

<sup>54</sup> Pièce R-6.

[142] L'hypothèse d'une faute contributive de chacun de ces groupes ne peut donc non plus être exclue à ce stade-ci, comme semblent l'avancer les demandeurs.

[143] La question est maintenant de savoir si ces fautes et manquements allégués d'Amazon peuvent engager la responsabilité de cette dernière directement envers les membres putatifs à qui appartiennent ces renseignements personnels.

[144] Amazon cherche à réduire et à limiter la portée de ses engagements pouvant découler d'une part, des représentations qu'elle formule sur son site web<sup>55</sup> et d'autre part, sur les obligations pouvant lui incomber envers autrui selon les lois provinciale et canadienne et par conséquent, en vertu de l'article 1457 du C.c.Q.

[145] En effet, ce n'est pas à Capital One, à première vue, mais bien aux membres putatifs et au public en général, qu'Amazon destine sa publicité et les informations qu'elle publie sur les services qu'elle rend au Canada en rapport à la sécurité du stockage des renseignements personnels pouvant lui être confiés sur ce territoire.

[146] Voici d'ailleurs les extraits du contenu du site web d'Amazon qui sont destinés aux résidents canadiens:

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.

[Le Tribunal souligne]

[147] Les engagements que l'on peut y lire sont clairs, précis et aussi étendus que ceux formulés dans les documents précités émanant de Capital One.

[148] Ainsi, il semble tout à fait concevable, selon un examen préliminaire des dispositions législatives en vigueur au Québec qui portent sur la protection des

---

<sup>55</sup> *Id.*



renseignements personnels, qu'Amazon puisse être assimilée à une personne qui détient des renseignements personnels appartenant aux membres putatifs, et ce, malgré l'absence d'un lien contractuel avec ceux-ci et qu'il en découle alors une responsabilité statutaire ou légale d'Amazon envers ces membres.

[149] Il est vrai que les allégations de la Demande révèlent qu'Amazon n'a souscrit formellement aucun engagement contractuel envers les demandeurs, ni envers les membres putatifs, mais le Tribunal reste cependant peu convaincu par l'argumentation d'Amazon sur la portée, particulièrement de la loi provinciale, à son endroit.

[150] Comme nous l'avons vu plus haut, les dispositions législatives précitées de la loi québécoise sur la protection des renseignements personnels dans le secteur privé, imposent des obligations à ceux qui détiennent de telles informations, sans préciser, ni limiter cette obligation uniquement à ceux qui ont conclu un contrat de service avec ces entreprises de services infonuagiques, et ce, contrairement à la LPC dont l'application se limite à un commerçant ayant conclu un contrat de consommation avec un consommateur et portant sur un bien ou un service.

[151] Or, l'article 3 de la loi québécoise sur la protection des renseignements personnels prévoit que la personne qui détient des renseignements personnels sur autrui « (...) doit prendre les mesures raisonnables pour diminuer les risques qu'un préjudice soit causé et éviter que de nouveaux incidents de même nature ne se produisent ».

[152] Pour sa part, l'article 10 de cette loi énonce que :

Toute personne qui exploite une entreprise doit prendre les mesures de sécurité propres à assurer la protection des renseignements personnels collectés, utilisés, communiqués, conservés ou détruits et qui sont raisonnables compte tenu, notamment, de leur sensibilité, de la finalité de leur utilisation, de leur quantité, de leur répartition et de leur support.

[153] De ces dispositions, il peut vraisemblablement en résulter un devoir d'Amazon envers les demandeurs et les membres putatifs, dont la violation peut correspondre à une faute statutaire ou extracontractuelle, dans ce dernier cas, commise en vertu de l'article 1457 C.c.Q. précité.

[154] Il est donc difficile pour le Tribunal d'écarter, à ce stade-ci, la possibilité que ces dispositions s'appliquent à Amazon et d'en limiter la portée uniquement à Capital One comme le suggère Amazon.

[155] En effet, selon Amazon, les dispositions du C.c.Q., et surtout celles de la loi provinciale précitée sur la protection des renseignements personnels, visent uniquement le principal responsable ou le gestionnaire des données recueillies ou la personne qui les contrôle.

[156] Amazon soutient que la responsabilité de Capital One en vertu de ces lois particulières demeure entière puisque cette dernière est le principal acteur dans la cueillette de ces renseignements personnels.

[157] Elle s'appuie en cela notamment sur des avis ou communiqués émis par le Commissariat canadien à la protection de la vie privée, et ce, en négligeant le fait que les renseignements personnels des membres en l'espèce aient été ensuite confiés par Capital One à Amazon, comme prestataire de services infonuagiques, et pour finalement conclure que seule Capital One doit supporter l'unique responsabilité du manquement à la sécurité informationnelle de ces renseignements personnels résultant de cet accès non autorisé.

[158] Le prestataire des services infonuagiques, en l'occurrence Amazon, ne pourrait donc encourir quelque responsabilité que ce soit à l'endroit des personnes à qui appartiennent ces renseignements du seul fait qu'ils ont été recueillis par Capital One auprès des membres.

[159] Or, Amazon ne cite aucune décision d'un tribunal canadien, ni aucune autre autorité pour soutenir une telle affirmation.

[160] En effet, les documents cités par Amazon dans sa plaidoirie et qui sont essentiellement des recommandations du Commissaire canadien à la vie privée s'adressant aux entreprises, organismes ou autres personnes obtenant les renseignements personnels et qui les confient à des tiers, indiquent que la personne à qui les données sont d'abord confiées demeure responsable et reste liée par cette obligation de sécurité informationnelle, ce qui semble parfaitement concevable et logique, mais surtout, cela est bien différent de ce que plaide Amazon puisque ces avis et recommandations ne suggèrent aucunement qu'un prestataire de services d'hébergement comme Amazon n'est aucunement responsable.

[161] La demande fait au surplus état d'une forme de partenariat<sup>56</sup> entre Capital One et Amazon dans le cadre duquel chacune a pu et peut encore tirer un avantage commercial et financier<sup>57</sup>, et aux termes duquel Capital One doit mettre à la disposition d'Amazon le plus grand nombre possible de renseignements personnels de ses clients, même plus anciens que ceux requis pour leurs opérations, afin qu'Amazon puisse, à l'aide ses propres serveurs et logiciels, mettre à profit d'autres outils d'intelligence artificielle visant à générer d'autres informations utiles à ses opérations commerciales et à celles de Capital One.

[162] Capital One et Amazon présentent d'ailleurs conjointement au public en 2016<sup>58</sup>, notamment sur leur site web respectif<sup>59</sup>, ce logiciel *Cloud Custodian*, devant pallier ou

---

<sup>56</sup> Par. 10.20 de la Demande.

<sup>57</sup> Par. 10.28.1 de la Demande.

<sup>58</sup> Par. 10.31.8.

<sup>59</sup> Par. 10.30 et pièce R-12.

solutionner la vulnérabilité alors connue ou alléguée des serveurs d'Amazon censés offrir la protection voulue.

[163] Amazon aurait même, selon les allégations de la Demande, encouragé cette migration massive des données recueillies par Capital One et jusque-là conservées par cette dernière, vers les serveurs d'Amazon, et la mise en place de ce procédé nommé *Cloud Custodian*<sup>60</sup>, conçu et implanté de concert avec Capital One, tout en rassurant les consommateurs canadiens que leurs serveurs locaux et l'architecture de leur réseau allaient satisfaire les exigences des organisations les plus sensibles à la sécurité informationnelle, pour ultimement fournir un environnement protégé à la disposition des consommateurs qui choisissent de recourir à leurs services locaux (canadiens) et ainsi satisfaire la réglementation fédérale en matière de protection des renseignements personnels<sup>61</sup>.

[164] Devant ces allégations, il n'est pas possible pour le Tribunal de minimiser le rôle d'Amazon, comme celle-ci le suggère, afin de limiter l'application et la portée en ce qui la concerne, des dispositions de la loi québécoise sur la protection des renseignements personnels et possiblement de la loi canadienne.

[165] Il existe donc une réelle possibilité que soit établie éventuellement qu'une ou plusieurs fautes extracontractuelles aient été commises par Amazon envers Royer et les membres putatifs.

[166] Subsidiairement, Amazon réfute la thèse des demandeurs selon laquelle, advenant un scénario où sa responsabilité extracontractuelle puisse être retenue, ce qu'elle nie vigoureusement, une condamnation solidaire puisse être prononcée contre toutes les défenderesses en l'instance, alléguant qu'en l'espèce, le recours dirigé Capital One est de nature contractuelle alors qu'il est de nature extracontractuelle contre Amazon, faisant en sorte qu'aucune solidarité entre ces deux groupes de défenderesses ne puisse être invoquée en vertu de l'article 1525 C.c.Q., si ce n'est qu'une responsabilité *in solidum*.

[167] À cette fin, les demandeurs tentent en effet d'assimiler Amazon à Capital One ou de les mettre sur le même pied vis-à-vis les membres, en invoquant leur connaissance commune dès 2018 de la vulnérabilité de leur système et de l'insuffisance des moyens déployés pour y suppléer, comme le *Cloud Custodian*.

[168] Le Tribunal souscrit, à première vue, aux prétentions d'Amazon en ce que les faits allégués dans la Demande et les pièces invoquées au soutien de celle-ci, ne soutiennent pas l'existence d'un lien de droit de même nature entre les membres d'une part, et Capital One et Amazon d'autre part.

---

<sup>60</sup> Par. 10.41 et pièces R-8, R-9 et R-10.

<sup>61</sup> Pièce R-6 en référence à la loi fédérale citée à la note 17.

[169] Ainsi, il semble bien que, préliminairement, on puisse conclure à une faute de nature extracontractuelle de la part d'Amazon, mais non pas à la possibilité d'une responsabilité solidaire de toutes les défenderesses entre elles et découlant de l'application à celles-ci de l'article 1525 C.c.Q. eu égard aux dispositions de la loi provinciale sur la protection des renseignements personnels et du C.c.Q.

[170] Le juge saisi du fond de l'affaire pourra éventuellement évaluer et devra déterminer ce qu'il en est de cette possible solidarité, sachant que la responsabilité de Capital One ne puisse être recherchée à la fois sur le plan contractuel et extracontractuel<sup>62</sup>.

### *Les représentations fausses ou trompeuses*

[171] Le Tribunal tient maintenant à préciser que les allégations de la Demande, en tenant celles-ci pour avérées à ce stade-ci des procédures, ne permettent aucunement d'établir l'apparence d'un recours basé sur des représentations fausses ou trompeuses de la part des défenderesses d'Amazon envers les membres, comme cette notion est définie à la LPC, selon le même raisonnement que celui appliqué ci-dessus à Capital One.

[172] Ces allégations des demandeurs s'appuient sur la prohibition de pratiques interdites en vertu de la LPC et pouvant entraîner une obligation de payer des dommages punitifs en vertu de l'article 272 de cette loi.

[173] Dans un premier temps, et cela nous apparaît déterminant ici, il n'y a aucune allégation suggérant qu'un contrat de consommation ait pu être conclu, de vente ou de location d'un bien ou de service, entre les demandeurs et les membres d'une part, et Amazon d'autre part.

[174] Il aurait pu ultimement être argué par les demandeurs que la responsabilité d'Amazon puisse être engagée sur la base uniquement de la commission d'une pratique interdite à laquelle elle se serait livrée, puisque dans ce cas la démonstration d'une pratique interdite n'est pas subordonnée à la conclusion d'un contrat<sup>63</sup>.

[175] Or, la pratique qui est interdite par la LPC consiste en celle d'un commerçant qui fait des représentations fausses ou trompeuses auprès d'un consommateur en vue de conclure un contrat de consommation avec celui-ci, ce qui ne peut être le cas d'Amazon dont les services sont destinés uniquement à Capital One, même si cela est au bénéfice ultime par ailleurs de la clientèle de cette dernière.

[176] Ainsi, de l'avis du Tribunal, il ne peut être valablement soutenu, même uniquement à ce stade de filtrage de la Demande, qu'Amazon ait pu engager sa responsabilité pour des représentations fausses ou trompeuses, comme définies à la

---

<sup>62</sup> Article 1458 C.c.Q.

<sup>63</sup> Article 217 LPC.

LPC, envers les demandeurs, ni les membres putatifs, car rien ne démontre, ni ne suggère qu'elle a conclu un contrat de consommation avec des membres, ni tenter de les inciter à le faire au moyen de pratiques interdites.

[177] Malgré les références faites par les demandeurs au site web d'Amazon, ils n'en infèrent aucunement, dans les allégations de leur Demande, qu'Amazon ait voulu ou cherché à conclure un contrat de consommation directement avec les membres.

[178] Par conséquent, rien ne supporte, à la face même de la Demande, la thèse que des représentations fausses ou trompeuses ont été faites par Amazon aux demandeurs ou aux membres putatifs, ni que la LPC lui soit applicable, laquelle doit donc être écartée dans le cas présent en ce qui concerne Amazon.

[179] De plus, tout comme c'est d'ailleurs le cas de Capital One, les demandeurs n'allèguent aucun fait précis démontrant la fausseté ou le caractère trompeur d'une représentation faite par Amazon, si ce n'est la survenance de cette intrusion dans son système d'hébergement de renseignements personnels, ce qui en soi peut constituer une faute extracontractuelle ou statutaire, comme discuté plus haut, mais cela ne démontre en rien la fausseté des représentations faites par Amazon sur les mesures de protection et de sécurité qu'elle a pu mettre en place.

e) Les dommages pécuniaires et non pécuniaires

[180] En ce qui concerne les dommages de cette nature pouvant être réclamés, rappelons qu'une jurisprudence particulière s'est développée au cours des dernières années en matière d'accès non autorisé à des renseignements personnels ou de vol de ceux-ci et d'identité, et pouvant être interprétée comme plutôt restrictive quant à la possibilité de réclamer de tels dommages.

[181] Il ressort de notre examen de cette jurisprudence que les faits allégués à la demande d'autorisation, doivent mettre en lumière une cause défendable et établir un préjudice compensable au stade de l'autorisation, de sorte que les dommages allégués doivent être davantage que ces ennuis ordinaires, ou que cette anxiété et la peur que peuvent vivre normalement les gens en de telles circonstances, les dommages incertains, futurs ou hypothétiques ne constituant pas un préjudice indemnisable.

[182] La Cour suprême a d'abord décidé dans l'affaire *Mustapha*<sup>64</sup> qui émane de l'Ontario, que le préjudice compensable par des dommages doit être plus important que de simples contrariétés :

[8] Règle générale, les tribunaux jugeront qu'un demandeur ayant subi un préjudice personnel a subi un dommage. Pour les besoins de la présente analyse, le terme dommage s'entend notamment d'un préjudice psychologique. En

---

<sup>64</sup> Préc. note 10.

matière de responsabilité délictuelle, la distinction entre préjudice physique et préjudice psychologique est difficile à cerner, voire artificielle (...) :

[TRADUCTION] En cette époque d'essor rapide des connaissances médicales, y compris en matière psychiatrique, il ne serait pas raisonnable d'astreindre les tribunaux à appliquer en droit une distinction entre préjudice physique et préjudice psychiatrique, distinction peut-être déjà quelque peu artificielle et qui pourrait, sous peu, être complètement dépassée. On ne gagne rien à les considérer comme des « catégories » différentes de préjudice à la personne et à forcer, de ce fait, l'application de critères juridiques différents.

[9] Cela dit, les troubles psychologiques constituant un préjudice personnel doivent être distingués d'une simple contrariété. En droit, un préjudice personnel suppose l'existence d'un traumatisme sérieux ou d'une maladie grave. Le droit ne reconnaît pas les contrariétés, la répulsion, l'anxiété, l'agitation ou les autres états psychologiques qui restent en deçà d'un préjudice. Je n'entends pas donner ici une définition exhaustive de ce qu'est un préjudice indemnisable, mais seulement dire que le préjudice doit être grave et de longue durée, et qu'il ne doit pas s'agir simplement des désagréments, angoisses et craintes ordinaires que toute personne vivant en société doit régulièrement accepter, fût-ce à contrecœur. Tout bonnement, les contrariétés mineures et passagères n'équivalent pas à un préjudice personnel et, de ce fait, ne constituent pas un dommage.

[Le Tribunal souligne] [Renvois omis]

[183] La Cour suprême explique ensuite que pour être indemnisable, un tel préjudice ne doit pas être trop éloigné :

L'analyse du caractère éloigné du préjudice dépend non seulement du degré de probabilité requis pour satisfaire à l'exigence de la prévisibilité raisonnable, mais également de la question de savoir si le demandeur est considéré d'un point de vue objectif ou subjectif. En l'espèce, il a notamment fallu se demander si, pour juger de la prévisibilité du préjudice personnel, il faut considérer la personne dotée d'une « résilience ordinaire » ou le demandeur concerné et ses vulnérabilités propres. Cette question peut être critique dans les poursuites pour préjudice psychologique, étant donné que les réactions individuelles face à des facteurs de stress particuliers peuvent varier considérablement d'une personne à l'autre. Il est de droit constant — dans le cadre de l'analyse de l'obligation de diligence doit-on préciser — que la question à trancher est celle de savoir ce qu'aurait supporté une personne dotée d'une résilience ordinaire

[184] Cette approche a été suivie au Québec, notamment dans l'affaire *Ly c. Equifax*<sup>65</sup> :

<sup>65</sup> *Li c. Equifax*, 2019 QCCS 4340.

[26] Rappelons que l'apparence de droit doit être étudiée à la lumière du cas personnel du demandeur.

[27] Selon les allégations de la Demande modifiée, le demandeur n'a pas été victime de vol d'identité ni n'a encore dépensé d'argent pour de l'achat de services de monitoring continuuel de crédit ni n'a encore subi de troubles et inconvénients associés entre autres à l'annulation de cartes de crédit et à l'organisation de services de monitoring de crédit. Le demandeur fait état de risque futur et de dépenses à venir. Il ajoute avoir subi un « mental distress ». Est-ce suffisant? Le Tribunal est d'avis que non. Voici pourquoi.

[28] Dans la décision *Zuckerman c. Target Corporation*, la Cour supérieure résume ainsi l'état du droit québécois sur les dommages dans des cas similaires :

[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] Ces propos font écho au concept selon lequel le risque de développer un préjudice futur, comme une maladie ou une infection n'est pas un dommage qui peut être compensé en droit québécois. Il s'agit d'un dommage incertain et hypothétique, interdit en vertu de l'article 1611 CcQ et des autorités pertinentes sur ce point. Un risque n'est pas un préjudice certain.

[30] Dans ces circonstances, le demandeur n'a pas d'apparence de droit pour les dommages suivants :

- Perte économique résultant entre autres de l'achat de services de monitoring continuuel de crédit;

- Troubles et inconvénients associés entre autres à l'annulation de cartes de crédit et à l'organisation de services de monitoring de crédit.

[31] De plus, le « mental distress » qu'allègue le demandeur n'est pas ici caractérisé ou décrit d'une façon qui lui permettrait de dépasser les désagréments, angoisses et craintes ordinaires que toute personne vivant en société doit régulièrement accepter, fût-ce à contrecœur. Il aurait fallu plus de détails que de simples allégations. Selon les allégations de la Demande modifiée, le Tribunal conclut que ce préjudice allégué par le demandeur est négligeable et n'a donc pas d'apparence de droit.

[32] Enfin, quant aux « autres pertes », aucune n'est alléguée par le demandeur. Il n'y a donc pas d'apparence de droit à cet égard.

[33] Le Tribunal note en terminant que le demandeur n'allègue pas avoir reçu une lettre de la part des défenderesses l'avisant d'avoir pu être potentiellement touché par l'incident de piratage, comme décrit aux Pièces D-1A, D-1B et D-2.

[34] Le Tribunal conclut que le demandeur n'a pas démontré de dommages compensatoires dans son cas personnel, ce qui signifie que l'action collective n'a pas d'apparence de droit et ne peut être autorisée pour cet aspect. Pour l'instant, le droit québécois ne reconnaît pas comme dommage compensatoire le simple fait que des renseignements personnels soient en possession non autorisée par des tiers, sans plus.

[Renvois omis]

[185] Au surplus, selon les défenderesses, la présente cause se distinguerait également d'autres affaires<sup>66</sup> où des dommages compensables ont été établis et dans lesquelles, selon la preuve offerte, une fraude résultant d'un vol de données avait été commise, ce qui ne serait pas le cas en l'espèce, comme en font foi les résultats de l'enquête tenue devant un tribunal pénal américain sur les faits et gestes posés par Paige A. Thompson, qui a conclu que celle-ci n'a pas ou n'a pas pu utiliser ces données obtenues illégalement.

[186] Les défenderesses avancent par conséquent que pour obtenir des dommages pécuniaires compensatoires, les demandeurs doivent établir que ceux-ci sont susceptibles d'évaluation ou quantifiables, de sorte que le Tribunal ne devrait pas tenir compte du risque d'un préjudice futur même si celui est allégué, puisqu'il ne peut être légalement compensé en droit québécois<sup>67</sup>.

[187] Essentiellement, les faits générateurs d'un droit d'action allégués par les demandeurs dans la présente affaire se limitent à cet accès illégal et non autorisé par Paige A. Thompson les 22 et 23 mars 2019 et dont l'enquête a révélé que, tout en

<sup>66</sup> Voir entre autres *Mazzona c. Daimler Chrysler Financial services canada inc.*, 2012 QCCS 958.

<sup>67</sup> Articles 1611 et 1613 C.c.Q.



admettant les gestes lui étant reprochés, elle n'aurait pas communiqué à qui que soit, ni utilisé de quelque façon que ce soit les renseignements personnels obtenus.

[188] Il n'y a aucune allégation spécifique formulée dans la Demande, ni même dans la quatrième modification de celle-ci, de la survenance d'un vol d'identité ou d'une difficulté quelconque découlant de cet accès non autorisé qui aurait pu entraîner un déboursé de la part des demandeurs, ni de démarches ou de déboursés effectués à la suite d'une utilisation illégale de renseignements personnels ou à la suite d'un vol de ceux-ci depuis les événements survenus en mars 2019.

[189] On ne peut bien sûr écarter cette crainte du risque qu'un autre accès ait lieu ou même, qu'il ait pu avoir lieu depuis 2019 et que des renseignements personnels aient été volés, puis distribués, mais non encore utilisés. Mais là encore, il s'agit de spéculation et d'hypothèses.

[190] Il n'y aurait donc, selon les défenderesses, aucun préjudice futur, direct et prévisible<sup>68</sup>, puisque celui invoqué est non seulement hypothétique et incertain, mais improbable et qu'il est difficile, voire impossible à évaluer.

[191] Les demandeurs prétendent quant à eux que la valeur globale du patrimoine respectif des membres et du leur se trouve affectée négativement du fait de cet accès non autorisé à leurs renseignements personnels, de même que leur cotation de crédit et que les coûts d'adhésion à cette carte de crédit sont devenus trop élevés puisqu'injustifiés.

[192] Les demandeurs invoquent à l'appui de leurs prétentions les statistiques obtenues par le Commissariat à la protection de la vie privée au Canada<sup>69</sup> ou provenant d'études ou de sondages effectués au Canada et aux États-Unis, en relation notamment avec le vol d'un numéro d'assurance sociale<sup>70</sup>.

[193] Or, outre le fait que cet accès semble n'avoir eu aucune suite tangible actuellement, le Tribunal croit fort difficile voire impossible d'évaluer une perte de valeur de ces renseignements avec la preuve qui lui est offerte, ni une perte correspondant à la réduction de la valeur des services offerts, ni aux risques associés à d'éventuelles difficultés à prévoir lors de demandes ultérieures de crédit.

[194] Voulant enfin être indemnisés pour le préjudice découlant de l'absence de diligence des défenderesses afin d'atténuer les conséquences possibles de cet accès non autorisé, les demandeurs reprochent à Capital One d'avoir attendu jusqu'au 29 juillet 2019 pour informer le public, par voie d'un communiqué, de la survenance de cet incident de confidentialité survenu quatre mois plus tôt, et que Capital One aurait pu être informée de cet incident avant le 17 juillet 2019.

---

<sup>68</sup> Articles 1611 et 1613 C.c.Q.

<sup>69</sup> Par. 10.73.5 et ss. de la Demande.

<sup>70</sup> *Id.* et par.10.73.7 et ss.

[195] Or, rien n'est allégué par les demandeurs sur l'impact réel d'un tel délai puisqu'à la suite de l'arrestation de Paige A. Thomson survenue le 28 août 2019, celle-ci n'avait pas encore utilisé ni reproduit les renseignements personnels obtenus, ni encore moins réussi à les vendre ou les distribuer.

[196] La question des coûts de surveillance nous semble devoir cependant faire l'objet d'une approche différente.

[197] Il semble en effet qu'il y a lieu ici de faire une distinction, comme l'a faite notre Cour dans l'affaire *Zuckerman c. Target Corporation* précitée, entre d'une part les vérifications aléatoires ou ponctuelles, ou même fréquentes et régulières des comptes bancaires et des relevés de leurs clients que les institutions financières peuvent effectuer à des fins de prévention et de surveillance de la fraude, même en l'absence d'un incident de confidentialité, comme celui survenu en l'espèce, puisque ces gestes font partie des opérations courantes des institutions financières et des services bancaires qu'elles offrent généralement à tous leurs clients sans facturation additionnelle, et d'autre part, cette vérification et la surveillance des comptes et relevés des clients à la suite d'une intrusion, services qui font ici l'objet de cette offre particulière par Capital One, d'une durée de deux ans, gratuitement, même si la preuve offerte dans le cas présent ne permet de faire une distinction particulière quant à la nature des vérifications effectuées.

[198] De plus, les services de vérification et surveillance offerts gratuitement en l'espèce ne découlent pas de l'utilisation de données, d'un vol de renseignements personnels ou d'une fraude, mais uniquement de la survenance de l'incident de confidentialité lui-même et des risques qu'elle comporte, malgré l'absence de conséquence connue vu les résultats de l'enquête concernant les agissements de Paige A. Thompson.

[199] Aussi, par le fait son offre de services de vérification et de surveillance, et sans égard à la suffisance de cette offre, Capital One semble reconnaître, en quelque sorte, qu'il s'agit d'une situation particulière nécessitant une telle surveillance des comptes et relevés de ses clients.

[200] Or, les demandeurs allèguent que cette période de deux ans leur permettant de bénéficier gratuitement de tels services de vérification et de surveillance, est manifestement insuffisante, une personne ne pouvant jamais vraiment, selon eux, en matière de vol de renseignements personnels, être à l'abri d'une fraude malgré le passage du temps, et ils invoquent plusieurs courriels reçus de membres putatifs à cet effet.

[201] Se pose donc ainsi finalement qu'une seule question, soit la suffisance de cette période de deux ans puisqu'il semble acquis que cette procédure de vérification et de surveillance soit nécessaire, à tout le moins utile, et qu'elle découle directement de cet incident de confidentialité.

[202] En effet, il peut s'agir d'un inconvénient plus qu'ordinaire, ce que devra apprécier le juge du mérite, et pouvant se prolonger sur une plus longue période que deux ans, et pouvant au surplus se traduire par un déboursé d'argent.

[203] Il pourrait être même suggéré que cette période de deux ans puisse être une norme suivie, connue et reconnue par les acteurs de l'industrie, et par voie de conséquence, tout aussi connue finalement par ces personnes malveillantes et mal intentionnées qui ne font qu'attendre simplement l'écoulement de cette période de deux ans connue dans l'industrie, avant de mettre leur méfait à exécution.

[204] Dans cette affaire *Zucherman c. Target Corporation*<sup>71</sup>, le juge Hamilton, maintenant à la Cour d'appel, a préféré laisser au juge du fond la question de déterminer si un déboursé de 19,95 \$ effectué par le représentant pour des frais de surveillance de son compte pouvait constituer un préjudice indemnisable.

[205] Dans l'affaire *Lévy c. Nissan*<sup>72</sup>, la Cour d'appel maintient le jugement de la Cour supérieure qui a considéré qu'il était plus indiqué et approprié, à l'instar du juge Hamilton, de faire déterminer par le juge du fond la possibilité de réclamer dans cette affaire des frais de surveillance des comptes bancaires, accordant le bénéfice du doute à la demande.

[206] Plus récemment, notre Cour autorisait une action collective dans laquelle il n'y avait aucune allégation de vol de données, mais uniquement de stress, de crainte et d'anxiété, notamment parce que les données avaient été rendues publiques.

[207] Des frais de surveillance des comptes bancaires étaient réclamés au motif que la période d'un an offerte gratuitement était alléguée comme étant insuffisante<sup>73</sup>, et l'autorisation d'exercer une action collective fut accordée.

[208] Au moment de l'instruction, cette période de surveillance gratuite de deux ans était vraisemblablement expirée et l'était probablement au moment de la quatrième modification de la Demande survenue le 25 avril 2022, même si celle-ci n'allègue pas que les demandeurs ou des membres ont dû payer des sommes d'argent pour prolonger cette période de vérification et de surveillance.

[209] Le Tribunal entend par conséquent ne reconnaître que ce seul chef de dommage comme apparaissant compensable au stade de l'autorisation, en laissant lui aussi au juge du fond toute la latitude, avec l'ensemble de la preuve qui sera administrée devant lui, pour décider ultimement si des coûts additionnels pour une période de vérification et surveillance plus longue que celle de deux ans offerte en l'espèce, peuvent constituer ici

---

<sup>71</sup> 2021 QCCA 682.

<sup>72</sup> *Id.*

<sup>73</sup> *Zucherman c. MGM Resorts International*, 2022 QCCS 2914.

un préjudice indemnisable, parce que raisonnablement prévisibles et découlant directement de la faute des défenderesses.

[210] Ainsi, sauf quant à ces frais additionnels de vérification et de surveillance pour une période supérieure à deux ans, les demandeurs ne démontrent l'existence d'aucun autre préjudice pécuniaire ou non pécuniaire subi à ce jour et pouvant correspondre à des frais engagés ou des pertes financières réellement encourues, ou encore des pertes financières ou des dépenses à venir et qui seraient elles aussi raisonnablement prévisibles.

f) Les dommages punitifs

[211] Les demandeurs réclament également des dommages punitifs et s'appuient à cette fin, tant sur l'article 49 de la Charte, en invoquant une atteinte intentionnelle à leur droit à protection de leur vie privée, que sur l'article 272 LPC.

[212] Comme discuté ci-dessus, la jurisprudence exige que l'intention des parties fautives soit prouvée de sorte que des allégations suffisamment claires et précises en ce sens doivent être formulées dans la Demande.

[213] Les demandeurs n'allèguent aucun fait précis démontrant qu'ils ont été l'objet d'une violation intentionnelle spécifique par les défenderesses de leur droit et de celui des membres à la protection de leur vie privée selon l'article 5 précité de la Charte.

[214] La Demande reproche plutôt à Capital One sa conduite négligente et peu soucieuse de la sécurité des renseignements personnels qu'elle a obtenus de ses clients, alors qu'elle savait ou devait savoir, lors de cette migration de cette masse imposante de renseignements personnels en 2015, que la protection et la sécurité de ces données pouvaient être affectées et éventuellement compromise parce que les mesures mises en place étaient inadéquates et insuffisantes.

[215] Selon les demandeurs, Capital One n'a pas respecté les normes et pratiques de l'industrie en matière de sécurité informationnelle, et ce, tout en accordant peu d'importance à la protection et à la sécurité des renseignements personnels de ses clients.

[216] Elle a privilégié son association potentiellement lucrative avec Amazon, en conservant à cette fin trop de données, incluant les membres dont le crédit fut refusé, et sur une trop longue période de temps, en allant de l'avant avec cette migration massive des renseignements personnels de ses clients vers un site d'hébergement public et reconnu pour être moins sécuritaire, puis en avisant tardivement les membres de cet incident de confidentialité et enfin, en ne remédiant pas à la vulnérabilité des mesures de protection et de sécurité mises en place.

[217] Selon l'auteur Me Claude Dallaire, devenue depuis juge à cette Cour, on observe à la lecture de la jurisprudence portant sur les atteintes attentionnelles à un liberté ou à

un droit reconnu par la Charte, qu'il est possible d'inférer une telle atteinte intentionnelle de la conduite d'une personne raisonnable qui, agissant de la sorte, ne peut ignorer les conséquences naturelles et immédiates que ses gestes peuvent générer :

L'intention est ce qu'on déduit des gestes de l'auteur de l'atteinte. Si le comportement choque, s'il est déraisonnable, s'il n'est pas justifié, s'il est grave ou répétitif, il y a de bonnes chances qu'on y trouve des éléments prescrits pour rencontrer le fardeau de preuve requis par la Cour suprême<sup>74</sup>.

[218] S'appuyant sur un arrêt de la Cour suprême, cette auteure poursuit en exposant qu'un plaignant a le fardeau de démontrer que la partie visée a agi de manière intentionnelle, malveillante ou vexatoire ou encore que sa conduite puisse se qualifier d'ignorance sérieuse ou de négligence atteignant ce niveau de gravité pour constituer une faute<sup>75</sup> :

Dans l'affaire *Gauthier c. Corporation municipale de Ville de Lac Brôme*, à peu près tous les indices ont été pris en considération par la Cour suprême pour lui permettre de conclure qu'il n'était pas possible qu'une personne raisonnable agissant de la sorte ne sache pas les conséquences naturelles et immédiates que ses gestes généraient ou qu'elle ne désire pas de telles atteintes à l'intégrité et à la dignité de la victime.

Selon notre compréhension, la Cour a utilisé le test du « savait ou devait savoir » pour démontrer l'intention des auteurs des diverses atteintes, tout particulièrement celle de la ville employeur. ...

À la lumière de ces exemples, on constate qu'il n'est pas difficile de rencontrer le fardeau de preuve requis pour l'octroi de dommages exemplaires sous la Charte québécoise. Il faut simplement comprendre ce qu'est l'intention à laquelle réfère l'article 49(2). L'intention est ce qu'on déduit des gestes de l'auteur de l'atteinte. Si le comportement choque, s'il est déraisonnable, s'il n'est pas justifié, s'il est grave ou répétitif, il y a de bonnes chances qu'on y trouve des éléments prescrits pour rencontrer le fardeau de preuve requis par la Cour suprême.<sup>76</sup>

[219] La Cour d'appel et notre Cour ont appliqué ces enseignements de la Cour suprême :

[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

---

<sup>74</sup> Préc., note 24.

<sup>75</sup> *Id.*

<sup>76</sup> *Id.*

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.<sup>77</sup>

[Le Tribunal souligne] [Renvois omis]

[220] Dans une affaire où certains reproches sont, à certains égards, comparables à ceux formulés en l'espèce, mais dont les faits diffèrent cependant, notre Cour a en effet décidé que<sup>78</sup> :

[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:

---

<sup>77</sup> Préc., note 25.

<sup>78</sup> *Zucherman c. MGM Resorts International*, 2022 QCCS 2914.

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;
- 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] Selon ces décisions, des inférences peuvent donc être faites par le Tribunal à partir de la conduite négligente et insouciante alléguée par la partie plaignante, pour conclure en une attitude répréhensible de l'autre partie, à l'égard de la confidentialité des renseignements personnels ainsi rendus accessibles.

[222] En définitive, le Tribunal doit apprécier, surtout à ce stade-ci de l'instance, si la trame factuelle, relatée ici de façon fort détaillée dans la Demande, démontre une conduite qui transcende l'importance de l'évènement survenu au mois de mars 2019 et qui n'en est que l'aboutissement, et qui peut préoccuper sérieusement, voire choquer un lecteur de ce récit, raisonnablement avisé et informé, tout en étant neutre et indépendant.

[223] Cette conduite comprend d'abord en l'espèce, selon la Demande, la masse colossale de données impliquées, dont certaines devenues inutiles et qui devaient possiblement être détruites rapidement, et d'autres qui furent conservées trop longtemps.

[224] Cette conduite doit aussi, selon le Tribunal, témoigner, au-delà de la faute commise, d'une attitude et d'une conduite téméraires de la part de Capital One, nonchalante et peu soucieuse envers l'importance de la protection de la vie privée lors de cette migration des renseignements personnels en 2015, cela tout en ayant une pleine

connaissance des risques qu'un bris de confidentialité puisse se produire et des conséquences sérieuses pouvant en résulter, comme le vol de renseignements personnels dans ce cas-ci, compte tenu des avis publiés, des sanctions obtenues et des alertes lancées.

[225] Cette conduite peut être encore plus choquante si la partie visée mise davantage sur l'intérêt commercial et financier pouvant provenir de l'utilisation de ces renseignements personnels, ce qui s'infère en l'espèce, de l'absence de diligence et de mesures réparatrices pour l'avenir une fois l'incident de confidentialité connu et sa cause, et alors que la déficience semble évidente par chacune de Capital One et d'Amazon qui s'accusent mutuellement d'être la cause de l'incident.

[226] La Demande allègue que Capital One et Amazon ont continué de suivre les mêmes procédures et mesures que celles en place depuis la migration des données vers Amazon, puis après l'incident survenu en mars 2019, sans corriger les lacunes de celui-ci<sup>79</sup>, ces allégations des demandeurs ne pouvant être qualifiées d'hypothétiques ou spéculatives et qui ne sont d'ailleurs pas contestées.

[227] La Demande allègue en effet que Capital One et Amazon n'ont rien fait, bien qu'alertées par différents acteurs de l'industrie, et ce qui devra être prouvé, pour prévenir et empêcher que l'incident de mars 2019 ne se produise, ni pour le contrecarrer ou pour éviter que cette situation ne survienne à nouveau dans l'avenir.

[228] Cette appréciation doit aussi tenir compte des attentes légitimes des membres envers une institution financière d'envergure, dont la réputation se mesure souvent à la hauteur de sa discrétion, sa réserve, sa prudence et son respect absolu de la confidentialité.

[229] C'est cette conduite, à tout le moins de façon *prima facie*, de la part de Capital One qui se dégage, étant celle auprès de qui les membres ont transigé, de sorte que les allégations de la Demande peuvent donner lieu, de l'avis du Tribunal, à l'octroi aux membres de dommages punitifs payables par Capital One en vertu des articles 5 et 49 de la Charte.

[230] Le Tribunal ne peut cependant tirer de telles conclusions sur la conduite d'Amazon dans cette affaire en raison de sa situation particulière vis-à-vis les membres.

[231] En effet, Amazon a certes fait des représentations publiques sur la protection qu'elle accorde aux renseignements personnels et au respect de la vie privée au Canada en vertu de la législation y étant applicable, mais ce n'est pas elle qui a sollicité cette clientèle, ni contracté avec les membres, ni recueilli ces renseignements personnels auprès de ceux-ci.

---

<sup>79</sup> Par. 10.59 de la Demande.



[232] Amazon, par les informations disponibles sur son site web, est une entreprise de service qui offre au public de l'hébergement de renseignements personnels.

[233] On ne peut donc pas examiner sa conduite en l'espèce, en ayant les mêmes standards que ceux que l'on peut considérer généralement applicables à une institution financière, comme c'est le cas de Capital One.

[234] En ce qui concerne l'application de l'article 272 LPC, les défenderesses soutiennent à bon droit que les demandeurs ne satisfont pas aux quatre critères énoncés par la Cour suprême dans l'affaire précitée *Richard c. Time inc.*<sup>80</sup>, lorsqu'elle nous propose ce cadre d'analyse quant à l'application de la LPC, ceci en raison de l'absence ici de représentations fausses ou trompeuses.

g) Conclusions du Tribunal sur l'article 575 al. 1 par. 2 C.p.c.

[235] Le Tribunal considère que le demandeur Abou-Khadra n'a pas fait la démonstration qu'il possède une cause défendable à faire valoir à l'encontre des défenderesses dans cette affaire.

[236] Toutefois, le Tribunal estime que le demandeur Royer a démontré l'existence d'une telle cause défendable à faire valoir à l'encontre de toutes les défenderesses, par lui et par tous les membres putatifs qui résident au Québec et qui ont été avisés de l'incident survenu les 22 et 23 mars 2019, soit une faute contractuelle par l'une, Capital One, et extracontractuelle par l'autre, Amazon, pour des dommages pécuniaires consistant en des frais de vérification et de surveillance des comptes et relevés des membres auprès de Capital One, pour une période supérieure à deux ans et qui devra être déterminée par le Tribunal.

[237] Cette cause d'action ne peut s'étendre toutefois à tous les dommages réclamés, ceux-ci devant se limiter, tout comme les questions communes à tous les membres, quant à toutes les défenderesses, à ces frais prévisibles de vérification et de surveillance de leurs comptes et relevés, auxquels s'ajoutent, quant aux défenderesses du Groupe Capital One, des dommages punitifs en vertu de l'article 49 de la Charte et devant être déterminés par le Tribunal.

[238] Enfin, la Demande propose une conclusion à être formulée dans l'action collective projetée enjoignant aux défenderesses de mettre en place des mesures de protection et de sécurité informationnelle adéquates pour prévenir et empêcher la survenance d'un nouvel accès non autorisé.

[239] Tel que cette conclusion de nature injonctive recherchée par Royer est actuellement formulée, elle est beaucoup trop vague, imprécise et générale pour qu'elle

---

<sup>80</sup> 2012 CSC 8.

soit éventuellement susceptible d'exécution, sachant les conséquences que la violation d'une ordonnance de la Cour peut entraîner.

[240] Le Tribunal ne la rejette cependant pas à ce stade-ci, préférant plutôt inviter le demandeur Royer à la reformuler dans sa déclaration introductive d'instance à être éventuellement déposée et notifiée à la suite du présent jugement, s'il souhaite toujours proposer ce débat particulier.

**III. Le critère prévu à l'article 575 al. 4 C.p.c. : les membres auxquels les demandeurs entendent attribuer le statut de représentants sont-ils en mesure d'assurer une représentation adéquate des membres putatifs?**

[241] À ce sujet, Amazon réitère que les demandeurs Royer et Abou-Khadra n'ont ni l'un ni l'autre, une cause d'action défendable à faire valoir contre elle puisque qu'ils n'ont aucun lien de droit avec Amazon, et alors que la Demande ne contient aucune allégation, ni preuve d'un préjudice indemnisable contre les défenderesses.

[242] Or, le Tribunal estime que le demandeur Royer a démontré qu'il possède une cause d'action défendable à faire valoir contre toutes les défenderesses, et dans le cas d'Amazon, sur le plan extracontractuel et à la lumière de l'application possible à celle-ci des dispositions de la loi québécoise sur la protection des renseignements personnels dans le secteur privé.

[243] Par conséquent, le Tribunal est d'avis, pour les motifs plus amplement développés ci-dessus, que seul le demandeur Michael Royer apparaît en mesure d'assurer une représentation adéquate des membres putatifs puisque, contrairement au demandeur Abou-Khadra, il fait partie de ces 6 000 000 de résidents canadiens avisés d'un accès non autorisé à ses renseignements personnels.

### **3. CONCLUSION**

#### **POUR CES MOTIFS, LE TRIBUNAL :**

[244] **ACCUEILLE** la demande du demandeur Michael Royer pour obtenir l'autorisation d'exercer une action collective contre les défenderesses Capital One Bank (Canada Branch) Capital (Financial Corporation) et Capital One Bank (USA) National Association et contre les défenderesses, Amazon.com inc., Amazon.com.ca inc., Amazon Web Services Canada inc., Amazon Web Services inc. et Amazon Technologies inc.;

[245] **REJETTE** la demande d'autorisation d'exercer une action collective introduite par le demandeur Ala'a Abou Khadra contre toutes les défenderesses;

[246] **DÉSIGNE** le Groupe des membres de la façon suivante :

«Toutes les personnes, entités ou organisations qui résident au Québec et qui ont détenu une carte de crédit émise par Capital One ou appliqué pour en obtenir une et dont les renseignements personnels ont fait l'objet d'un accès non autorisé les 22 et 23 mars 2019».

[247] **DÉSIGNE** le demandeur Michael Royer à titre de représentant des membres qui font partie du Groupe;

[248] **IDENTIFIE** comme suit les questions communes devant être débattues dans le cadre de cette action collective :

- a) Les défenderesses du groupe Capital One ont-elles été fautives envers les membres en vertu du contrat liant les parties en ce qui concerne la protection et la sécurité de leurs renseignements personnels depuis 2004, lors de cette migration de leurs renseignements personnels vers les serveurs des défenderesses Amazon en 2015 et par la suite?
- b) *La Loi sur la protection des renseignements personnels et les documents électroniques s'applique-t-elle aux défenderesses?*
- c) Les défenderesses du groupe Capital One et du groupe Amazon ont-elles été fautives envers les membres en vertu de la *Loi sur la protection des renseignements personnels dans le secteur privé* et en vertu de la *Loi sur la protection des renseignements personnels et les documents électroniques* entre 2004 et la date de la présente instance?
- d) Les défenderesses du Groupe Capital One et du Groupe Amazon sont-elles tenues de payer aux membres des coûts pour la surveillance de leurs comptes et relevés de leurs cartes de crédit Capital One pour une durée supérieure à deux ans, et dans l'affirmative, déterminer ces coûts pouvant être réclamés?
- e) Les défenderesses du groupe Capital One ont-elles porté atteinte au droit à la vie privée des membres en vertu de la *Charte des droits et libertés de la personne*?
- f) Les défenderesses du groupe Capital One sont-elles tenues à des dommages punitifs aux membres et, dans l'affirmative, pour quel montant?

[249] **IDENTIFIE** les conclusions recherchées de la façon suivante :

- **ACCUEILLIR** l'action collective intentée par le demandeur Michael Royer contre toutes les défenderesses;
- **DÉCLARER** que les défenderesses Capital One Bank (Canada Branch) Capital (Financial Corporation) et Capital One Bank (USA) National

Association ont commis une ou plusieurs fautes contractuelles envers les membres;

- **DÉCLARER** que les défenderesses Capital One Bank (Canada Branch) Capital (Financial Corporation) et Capital One Bank (USA) National Association, Amazon.com inc., Amazon.com.ca inc., Amazon Web Services Canada inc., Amazon Web Services inc. et Amazon Technologies inc. ont enfreint la *Loi sur la protection des renseignements personnels dans le secteur privé* et la *Loi sur la protection des renseignements personnels et les documents électroniques*;
- **DÉTERMINER** le montant des coûts requis pour la surveillance des comptes et relevés des cartes de crédit des membres, pour une durée raisonnablement prévisible, comme conséquence des événements survenus les 22 et 23 mars 2019, et **CONDAMNER** les défenderesses, solidairement, à payer aux membres le montant de ces coûts;
- **DÉCLARER** que les défenderesses Capital One Bank (Canada Branch) Capital (Financial Corporation) et Capital One Bank (USA) National Association, ont porté atteinte au droit à la vie privée des membres du Groupe garanti par l'article 5 de la *Charte des droits et libertés de la personne*, et **CONDAMNER** ces dernières, solidairement, à payer aux membres une somme à être déterminée par le Tribunal à titre de dommages punitifs en vertu de l'article 49 de la *Charte des droits et libertés de la personne*, avec les intérêts au taux légal et l'indemnité additionnelle prévue à la Loi;
- **ORDONNER** le recouvrement collectif des réclamations des membres du Groupe ou à défaut, le recouvrement individuel de celles-ci;
- **LE TOUT** avec dépens contre les défenderesses, incluant tous les frais d'expert et de publication des avis requis par la Loi;

[250] **DÉCLARE** que sauf exclusion, tous les membres du Groupe seront liés par tout jugement à intervenir sur l'action collective de la manière prévue à la loi;

[251] **FIXE** à trente (30) jours suivants de la date du présent jugement, la période pendant laquelle un membre peut demander son exclusion, à la suite de laquelle tous les membres du Groupe qui n'auront pas demandé leur exclusion seront liés par le jugement à être rendu sur l'action collective;

[252] **ORDONNE** la publication d'un avis de la présente action collective aux membres accessibles du Groupe en vertu de l'article 579 C.p.c. et rédigé de la façon appropriée;

[253] **ORDONNE** aux défenderesses d'envoyer cet avis aux membres du Groupe à leur dernière adresse courriel connue avec la mention « Avis d'action collective » dans l'objet du courriel;

[254] **ORDONNE** aux défenderesses de publier cet avis aux membres du Groupe sur leur site web, leur page Facebook ou Threads, leur page Twitter, avec la mention « Avis d'action collective » pendant trente (30) jours suivants le présent jugement;

[255] **ORDONNE** que la date de fermeture du Groupe soit celle de la publication de l'avis aux membres;

[256] **LE TOUT** avec les frais de justice contre les défenderesses.

---

**BERNARD TREMBLAY, j.c.s.**

M<sup>e</sup> Jeff Orenstein  
M<sup>e</sup> Andrea Grass  
CONSUMER LAW GROUP INC.  
Avocats des demandeurs

M<sup>e</sup> Noah Boudreau  
M<sup>e</sup> Mirna Kaddis  
FASKEN MARTINEAU DUMOULIN INC.  
Avocats des défenderesses Capital One Bank (Canada Branch), Capital (Financial Corporation) et Capital One Bank (USA) National Association.

M<sup>e</sup> Paule Hamelin  
GOWLING WLG (CANADA)  
Avocate des défenderesses Amazon.com inc., Amazon.com.ca inc., Amazon Web Services Canada inc., Amazon Web Services inc. et Amazon Technologies inc.

Dates d'audience : 31 janvier et 1<sup>er</sup> février 2023