IN THE SUPREME COURT OF BRITISH COLUMBIA

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

Date: 20220603
Docket: S198617
Registry: Vancouver

Between:

Duncan Campbell

Plaintiff

And

Capital One Financial Corporation, Capital One Bank (USA), National Association, and Capital One Bank (Canada Branch)

Defendants

Before: The Honourable Justice Iyer

Reasons for Judgment

Counsel for Plaintiff:	T. Charney R. Loeb C. Edwards K. Garcha P. Sanghe
Counsel for Defendants:	L. Cooper A. Cameron A. Borrell V. Toppings P. Sergeyev
Place and Date of Trial:	Vancouver, B.C. January 31, February 1-3, 2022
Place and Date of Judgment:	Vancouver, B.C. June 3, 2022

Table of Contents

OVERVIEW

[1] Capital One issues credit cards for its banking business as well as for Costco Wholesale and the Hudson's Bay Company. When applying for such a credit card, individuals provide Capital One[1] with their personal and financial information. Capital One stores that information in a database on Amazon Web, a third party cloud-based server in the United States. In the spring of 2019, Paige Thompson hacked Capital One's database. She downloaded the personal and financial information of American and Canadian residents who had applied for Capital One credit cards ("Data Breach"). The Data Breach affected six million Canadian customers and about 100 million American customers.

[2] In July 2019, an independent security researcher discovered the breach and informed Capital One, which contacted American law enforcement. FBI agents arrested Ms. Thompson and seized digital devices from her home on July 29, 2019. On the same day, Capital One published a statement about the cyber-breach on its website.

[3] The data stolen from Canadians included information submitted on credit card applications between 2005 and early 2019, such as name, date of birth, mother's maiden name, address, email address, phone number, employer name, housing situation, annual income, status of mortgage, and banking information. It included some people's credit scores, credit limits, balances and payment history, and fragments of transaction histories over a total of 23 days in 2016-2018. The Data Breach also compromised about one million social insurance numbers. I will refer to all of this information as the "Confidential Information".

[4] Capital One wrote to all affected individuals to notify them of the Data Breach. It explained what steps they could take to monitor and protect their data and offered them free credit monitoring and identity protection services, including identity theft

[1] The defendants are Capital One Financial Corporation, Capital One Bank (USA) National Branch ("COBNA") and Capital One Bank (Canada Branch). I will refer to them collectively as "Capital One" unless necessary to identify them individually.

protection for two years. It stated that no credit card numbers, PIN codes or login credentials were compromised in the Data Breach.

[5] Legal proceedings commenced in the United States and in Canada. Ms. Thompson was criminally charged in the US and at the time of the hearing before me, was awaiting trial. At the end of July 2019, the Office of the Privacy Commissioner of Canada ("OPC") announced it was commencing an investigation. As of this date, the OPC has not issued a report. In August 2020, the US Office of the Comptroller of Currency found Capital One non-compliant with its risk assessment standards and imposed civil penalties totaling USD $80 million.

[6] In Canada, national class actions were commenced in British Columbia, Alberta, and Ontario. There were carriage contests in British Columbia and Ontario. Perrell J. of the Ontario Superior Court granted carriage to the *Del Giudice* action in Ontario (*Del Giudice v. Thompson*, 2020 ONSC 2676) and I granted carriage to Mr. Campbell here: *Campbell v. Capital One Financial Corporation*, 2020 BCSC 1696. It does not appear that the Alberta claims are proceeding. A class action was filed in Québec on behalf of a Québec class. As discussed further below, that action is being case managed by Justice Bernard Tremblay. Most recently, Perell J. dismissed the plaintiff's application for certification in *Del Giudice*: 2021 ONSC 5379. I am informed that his decision is under appeal and will be heard in June 2022.

[7] There is no evidence as of the date of this certification hearing that any of the Confidential Data has been disseminated beyond Ms. Thompson. Capital One's primary objection to certification is that the absence of such evidence means that the action cannot be certified.

THE TEST FOR CERTIFICATION

[8] Sections 4(1) and (2) of the *Class Proceedings Act*, R.S.B.C. c. 50 [*CPA*], set out the requirements for certifying a class proceeding:

> 4 (1) Subject to subsections (3) and (4), the court must certify a proceeding as a class proceeding on an application under section 2 or 3 if all of the following requirements are met:

> (a) the pleadings disclose a cause of action;
>
> (b) there is an identifiable class of 2 or more persons;
>
> (c) the claims of the class members raise common issues, whether or not those common issues predominate over issues affecting only individual members;
>
> (d) a class proceeding would be the preferable procedure for the fair and efficient resolution of the common issues;
>
> (e) there is a representative plaintiff who
>
> > (i) would fairly and adequately represent the interests of the class,
> >
> > (ii) has produced a plan for the proceeding that sets out a workable method of advancing the proceeding on behalf of the class and of notifying class members of the proceeding, and
> >
> > (iii) does not have, on the common issues, an interest that is in conflict with the interests of other class members.
>
> (2) In determining whether a class proceeding would be the preferable procedure for the fair and efficient resolution of the common issues, the court must consider all relevant matters including the following:
>
> > (a) whether questions of fact or law common to the members of the class predominate over any questions affecting only individual members;
> >
> > (b) whether a significant number of the members of the class have a valid interest in individually controlling the prosecution of separate actions;
> >
> > (c) whether the class proceeding would involve claims that are or have been the subject of any other proceedings;
> >
> > (d) whether other means of resolving the claims are less practical or less efficient;
> >
> > (e) whether the administration of the class proceeding would create greater difficulties than those likely to be experienced if relief were sought by other means.

[9] The settled principles governing the certification analysis are succinctly summarized by Justice Francis in *Sharifi v. WestJet Airlines Ltd*., 2020 BCSC 1996 rev'd on other grounds 2022 BCCA 149:

> [12] The certification requirements are to be interpreted generously, taking into account the objects of class action legislation and the perceived benefits of such proceedings: *Gary Jackson Holdings Ltd. v. Eden,* 2010 BCSC 273 at para. 28.

> [13] The class procedure has three principal goals: behaviour modification, judicial economy and access to justice: *Hollick v. Toronto (City)*, 2001 SCC 68 at para. 27.
>
> [14] The certification analysis does not involve a consideration of the merits of the claim. The question at certification is not whether a claim is likely to succeed but rather whether the suit is appropriately brought as a class proceeding: *Hollick* at para. 16.
>
> [15] Subsection 4(1)(a), the requirement that the pleadings disclose a cause of action, is assessed by means of the same test that would apply to a motion to strike. A plaintiff will satisfy this requirement unless, assuming all the facts pleaded to be true, it is plain and obvious that the plaintiff's claim cannot succeed or has no reasonable prospect of success: *Pro-Sys Consultants v. Microsoft Corporation*, 2013 SCC 57 at para. 63 [*Pro-Sys*].
>
> [16] With respect to the remaining subsections 4(b) – (e), the plaintiff must show "some basis in fact" to establish that the certification requirements have been met. In determining whether this standard has been met, the court should not engage in any detailed weighing of evidence at the certification stage but should confine itself to whether there is some basis in the evidence to support the certification requirements: *AIC Limited v. Fischer*, 2013 SCC 69 at para. 43.

[10] In *Sherry v. CIBC Mortgage Inc.*, 2020 BCCA 139, the Court of Appeal confirmed that, for purposes of the s. 4(1)(a) analysis, pleaded facts must be assumed to be true unless they are patently unreasonable or incapable of proof, and the claim's prospect of success must be reasonable, not speculative: at paras. 23-24. Dickson J.A. added that certification judges should not shy away from deciding challenging legal questions: at para 25.

[11] In *Atlantic Lottery Corp. Inc. v. Babstock*, 2020 SCC 19 at para. 19 [*Babstock*], the Court cautioned that, while novel claims that might represent an incremental development in the law should be allowed to proceed to trial, "[i]t is beneficial, and indeed critical to the viability of civil justice and public access thereto that claims, *including novel claims*, which are doomed to fail be disposed of at an early stage in the proceedings." (Emphasis in original.) This is because such claims present "no legal justification for a protracted and expensive trial".

[12] Recently, in *Trotman v. WestJet Airlines Ltd.*, 2022 BCCA 22, Bauman C.J. addressed the gate-keeping role of a certification judge where there is a question of statutory interpretation (at para. 46). The judge should not engage in a merit-based analysis unless there is previous binding case law on the point or "the interpretive

exercise is so straightforward the answer is plain and obvious even without previous case authority.

[13] With respect to the “some basis in fact” assessment, in *676083 B.C. Ltd. v. Revolution Resource Recovery Inc*., 2021 BCCA 85 at para. 31, the Court of Appeal underscored that the certification stage serves an important gate-keeping function:

> Section 4(1) of the *CPA* establishes the statutory requirements for certification of a class action. When these requirements are met, the proceeding must be certified. The merits of a claim are not determined on a certification application and the threshold for certification is low. Nevertheless, certification serves as a "meaningful screening device", and the court performs "an important gatekeeping role by screening out those claims destined to founder at the merits stage of the proceeding": *Pro-Sys Consultants Ltd. v. Microsoft Corporation*, 2013 SCC 57 at paras. 103─104 [*Pro-Sys Consultants*]; *Sherry* at para. 22. Thus, the standard for assessing evidence at certification requires more than a "superficial level of analysis into the sufficiency of the evidence" and more than "symbolic scrutiny": *Pro-Sys Consultants* at para. 10.

[14] These principles guide my analysis.

THE CERTIFICATION APPLICATION

[15] The certification application seeks certification of a single national class comprised of all Canadians who Capital One informed that their Confidential Information was affected by the Data Breach (“Class”). Mr. Campbell seeks appointment as the representative plaintiff for the Class.

[16] The application proposes 27 liability-related common issues. These advance causes of action in negligence, breach of contract and warranty, breach of the duty of honest performance, breach of confidence, intrusion upon seclusion, breach of statutory privacy rights, breach of consumer protection statutes, and breach of the *Civil Code of Québec* [*CCQ*]. Five remedial common issues are proposed, addressing issues such as joint and several liability, whether damages can be assessed in the aggregate, responsibility for costs of distribution of awarded damages, and interest. The Amended Notice of Civil Claim filed January 10, 2022 (“Claim”) quantifies damages at $800 million.

UNDISPUTED FACTS

[17] Many of the background facts are not disputed. Rather, the parties disagree about how they should be interpreted and how they affect the issues I must decide.

Capital One's Promises to Safeguard Personal Information

[18] All Class members applied for Capital One credit cards between 2005 and 2019. To do so, they had to fill out an online application form ("Application"), providing the following information:

> Name
> Date of Birth
> Mother's Maiden Name
> Social Insurance Number [Optional]
> Address
> Email Address
> Phone Number
> Employment Status
> Housing situation [Optional]
> Annual Income before taxes
> Other Income before taxes
> Monthly Mortgage/Rent payment
> Whether they have any bank accounts

[19] The Application informed applicants that by clicking "Review my Application" they were confirming they had read Capital One's "Important Disclosures", "About Your Privacy", and "Other Important Information", all of which were hyperlinked to the Application.

[20] This material stated, in relevant part:

> Terms of Offer
>
> By submitting the Application Form, the applicant ("I"):
>
> 1. Certify that the information provided is true and correct and understand that Capital One Bank (Canada Branch), ("Capital One"), will rely on this and other information in deciding to open a MasterCard Account ("Account");

2. Request that Capital One open an Account and issue appropriate MasterCard card(s) ("Card(s)") and Personal Identification Number(s) to me (including renewals and replacements from time to time);

3. Request that Capital One issue appropriate Cards to me for any Authorized User identified on the Application Form, as well as renewals and replacements from time to time;

4. Agree that use of the Account or Card(s) will confirm acceptance of Capital One's MasterCard Customer Agreement as amended from time to time (the "Agreement"), which will be sent with my Card(s) if approved; …

[21] Under the heading, “Privacy Terms”, the Application stated as follows:

Privacy Terms

We respect your privacy. Not only do we respect it, but we also protect it. We collect and provide your information as required for the standard operation of our business and as required by law. We may also release your information to companies that you have authorized us to release your information to, including service providers (such as the printers of our account statements), credit reporting agencies (like TransUnion and Equifax), our own affiliates and co-branding partners for cobranded rewards card. These companies must first meet our rigorous privacy standards before we partner with them to do business for you. We will not add your name to third-party marketing campaigns for the first 30 days after the opening of your account to give you an opportunity to make your privacy choice known to us. You can tell us your privacy preferences by writing to us at the following address:

…

We may collect information about consumers who are not our current customers, so we can develop our products and services. Sometimes this information comes from lists like the telephone book. When a consumer applies to be our customer, we collect the information given during the application process (such as the consumer’s name, address, telephone number and date of birth). We want you to understand why we collect and use information about you and how this can benefit you. By knowing more about our customers, we and our business partners can provide specialized products that may be of interest to you and your family. We collect and use information about consumers and customers so we or our service vendors (whether engaged by or on behalf of us or any of our assignees) can use it in the following ways:

i. to open, maintain, service, process, analyze, survey, audit, and collect on an account;

ii. to verify your identity and credit worthiness;

iii. to protect you from identity theft, fraud, and unauthorized access to your account;

iv. to share application and transaction information with consumer reporting agencies and other parties who have financial, employment or business dealings with you;

v. to determine your eligibility, administer and contact you for the purposes of marketing, promotions, rewards programs, research or contests; and

vi. to use for any purpose required by law.

In addition, we may use your information in order to identify your preferences and determine your eligibility for special offers and discounts, if approved, or to make another offer to you or analyze your application (including your credit reports) even if you are declined for this application. This information may also be shared with any person or entity to which we have assigned or transferred an interest in your account or any debt or interest due under the terms to be provided in the Customer Agreement. This will apply upon your approval, and/or any of our rights and obligations under the Customer Agreement, including any subsequent assignee or transferee.

We may contact you by e-mail using the e-mail address you provided for special offers or standard service messages. To ensure your security, we will not include sensitive information in an e-mail such as your full 16-digit account number, date of birth, Social Insurance Number (if provided) or account balance. In the event that a service vendor is located outside of Canada, the information on file for you or an authorized user may be processed and stored outside Canada and foreign governments, courts of law enforcement or regulatory agencies may be able to obtain disclosure of this information. If you apply for credit, or by communicating or providing information to us in any other way, you acknowledge your consent for personal information collection, protection, use, disclosure and retention as set out herein. Subject to legal and contractual restrictions, you may withdraw your consent at any time after your account has been opened with reasonable notice.

Privacy Terms for Authorized Users

We or our service vendors (whether engaged by or on behalf of us or any of our assignees) may collect, use and disclose personal information of authorized users such as name and details of their transactions to: open, maintain, service, process, analyze, audit and collect on the account (notwithstanding that authorized users will not be held liable for the account); protect the account from identity theft, fraud and unauthorized access; and for any purpose required by law. All information on file for authorized users may be disclosed to the applicant. All information may also be shared with any person or entity to which we have assigned or transferred an interest in the account, or any debt or interest due under the terms to be provided in the Agreement, if approved, and/or any of our rights and obligations under the Agreement (including any subsequent assignee or transferee).

If you want to learn more about our privacy policies, please call us toll-free at 1-800-481-3239 or review the Capital One Privacy Statement included in the Customer Agreement you will receive as part of your Welcome Kit.

…

> Personal Use
>
> You agree that you will use your Card and your Account for personal, family or household purposes only and will not use your Card or your Account for any other purpose, including for business or commercial purposes.

[22] I will refer to the information about privacy in the Application as the "Privacy Terms".

[23] If Capital One approved the Application, it issued the credit card and sent it to the person with a cardholder agreement ("Agreement") that included the following relevant terms:

> Customer Agreement
>
> We're happy to open your credit card account. This Agreement contains information about your account. Please read it and keep it for your records. In this Agreement, the words "you," "your" and "yours" refer to the applicant and any co-applicant who, according to our records, was identified as such as part of the application, meaning the request to us for the account. These words do not include an authorized user. The words "we," "us" and "our" mean the Capital One® Bank (Canada Branch) and its successors or assigns. The word "transaction" means purchases, cash advances, special transfers, balance transfers, Account Access Cheque use, credits, mail or phone orders, or any other use of the account. The provisions of the Initial Disclosure Statement that you received when we approved your application for a Capital One credit card and the terms of our Privacy Statement, as well as amendments to either that we provide to you, are incorporated as part of the terms of this Agreement.
>
> 1. Confirming your Agreement with us.
>
> When your account is accessed for the first time, it confirms the account was opened at your request, that you accept the terms of this Agreement and that you request renewal replacement cards and Account Access Cheques. Where you have requested a personal identification number (PIN), its first use also confirms this Agreement's terms concerning it.
>
> ….
>
> Privacy Statement
>
> Our Commitment to Protecting Your Privacy
>
> Capital One® is committed to keeping your personal information accurate, confidential and secure. We want to earn your trust by providing strict safeguards to protect your information.
>
> What is Personal Information?
>
> Personal information is any information that can identify you.

Your Privacy

We respect your privacy. Not only do we respect it, but we also protect it. The personal information you share with us, stays with us. We collect and provide your information as required for the standard operation of our business and as required by law. We may also release your information to companies that you have authorized us to release your information to, including service providers (such as the printers of our account statements), credit reporting agencies (like TransUnion and Equifax), our own affiliates and co-branding partners for co-branded rewards card. These companies must first meet our rigorous privacy standards before we partner with them to do business for you.

Your Privacy Choices and How to Contact Us

We will not add your name to third-party marketing campaigns for the first 30 days after the opening of your account to give you a opportunity to make your privacy choice known to us.

…

Access to Personal Information about You

We retain your personal information on our servers and hard drives or on those of our service providers, both within and outside of Canada. You may request access to the personal information we collect about you. …

Confidentiality and Security

We have physical security (access in buildings), electronic protection (encryption), and safe business practices (customer authentication when you call us) to prevent identity theft. We restrict access to your personal information to those who need to have it to provide products or services to you. We use other companies to provide services for us such as marketing, advertising and credit card embossing, but select these companies carefully and require them to keep the information we share with them safe and secure. We do not allow them to use or share information for any purpose other than the job they are hired to do.

…

Use of Information

We want you to understand why we collect and use information about you and how this can benefit you. By knowing more about our customers, we and our business partners can provide specialized products that may be of interest to you and your family. We collect and use information about consumers and customers so we or our service vendors (whether engaged by or on behalf of us or any of our assignees) can use it in the following ways:

> (i) to open, maintain, service, process, analyze, survey, audit and collect on your account;
>
> (ii) to verify your identity and credit worthiness;
>
> (iii) to protect you from identity theft, fraud and unauthorized access to your account;

> (iv) to share application and transaction information with consumer reporting agencies and other parties who have financial, employment or business dealings with you and;
>
> (v) to determine your eligibility, administer and contact you for the purposes of marketing, promotions, rewards programs, research or contests; and
>
> (vi) to use for any purpose required by law.
>
> This information may also be shared with any person or entity to which we have assigned or transferred an interest in your account, any debt or interest due or any of our rights or obligations under any agreement with you (including any subsequent assignee).
>
> …
>
> Sharing of Information
>
> …
>
> Other third parties. We may share with carefully selected business partners information we collect about our customers, former customers, and withdrawn or declined applicants, such as name, street address, e-mail address and telephone number, for the purpose of determining the eligibility of customers and consumers for valuable products and services (such as credit balance insurance and credit report monitoring) offered by us or our business partners. We may share customer information with other parties who have financial, employment or business dealings with you. If you give us your Social Insurance Number, we may use it to identify you with credit reporting agencies and other parties, and we may keep it along with other information about you in our records, even after your account is closed to use for the purposes stated above. We ensure that any third party is bound to respect your privacy rights in the same way that we are.
>
> …
>
> Your Consent
>
> If you apply for credit, or by communicating or providing information to us in any other way, you acknowledge your consent for personal information collection, protection, use, disclosure and retention as set out herein. Subject to legal and contractual restrictions, you may withdraw your consent at any time after your account has been opened with reasonable notice.

[24] I will refer to the terms respecting privacy in the Agreement as the “Privacy Statement”.

[25] Capital One also had a privacy policy (“Privacy Policy”) that was incorporated by reference into the Agreement. In material part, it provided as follows:

> 1. PRIVACY COMMITMENT AND PERSONAL INFORMATION
>
> Capital One® is committed to keeping personal information accurate, confidential and secure.

> We collect, use and disclose personal information to operate our business and as required by law. Personal information is information about an identifiable individual, as defined in the Personal Information Protection and Electronic Documents Act.
>
> 2. CHANGES TO PRIVACY POLICY
>
> This Privacy Policy ("Policy") describes our current privacy practices. We update this Policy on an ongoing basis to ensure consumers, applicants and customers are aware of updates to our privacy practices, to streamline those practices and to comply with applicable laws. Consumers are individuals who are not currently our customers; applicants are individuals who apply to become our customers; and customers are individuals who have been approved, use or have used our products and services in the past. Please visit this site regularly for updates.
>
> …
>
> 4. IDENTIFYING PURPOSES
>
> Capital One clearly identifies the purposes for which personal information is collected, used or disclosed prior to or at the time of collection.
>
> Capital One may collect, use and disclose personal information of consumers, applicants and customers to develop, analyze and advertise products and services, process applications, maintain and service accounts, and comply with applicable laws.
>
> Except where information is marked as mandatory, you get to decide what information you want to share with us.

[26] In ensuing paragraphs, the Privacy Policy explains what information it collects from consumers, applicants and customers, and how it uses such information. It states the following with respect to consent:

> 5. CONSENT
>
> If you apply for a credit product, communicate with us or provide personal information to us in any way, you acknowledge your consent for personal information collection, use and disclosure as set out in this Policy or applicable laws and industry standards. If we want to use your information for a purpose that was not disclosed at the time of initial consent, consent will be sought at the time of this new purpose.
>
> **Updating consent.** 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 Capital One. You can also request that we don't contact you for advertising, marketing, promotions, rewards programs, research or contests; however, we may still need to contact you to comply with applicable laws or for business needs.

[27] Under the heading “Limiting Use, Disclosure and Retention”, Capital One states:

> Capital One limits use, disclosure and retention of personal information to the purposes we identify, and as required by applicable laws.
>
> **Third-party service providers.** We may share your personal information with service providers who perform services on our behalf (such as credit reporting, marketing, research, data processing and other services as required to service you). Our contracts with third parties include obligations to protect your personal information, and third parties must meet our rigorous privacy standards. When you engage with other companies directly, or contact us through their platforms, their use of the information they collect from you is subject to the terms of their privacy policies.
>
> …
>
> **Information processed outside Canada**. 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 Canada, foreign governments, courts or regulatory agencies may therefore be able to obtain such personal information through the laws of the foreign jurisdiction.

[28] This section does not address retention other than in its opening clause.

[29] The Privacy Policy describes how it protects personal information:

> Capital One uses procedures and practices appropriate to the sensitivity of personal information to protect against loss, theft and unauthorized access. Access to your information is restricted to those individuals and parties who require access.
>
> For example, we have physical security (such as restricted access to our offices and secure storage), electronic protection (such as passwords and encryption) and safe business practices (such as customer authentication when you call us). We also train our staff on how to safeguard personal information.
>
> You can help us safeguard your information too. If you contact us through email or social media, you should avoid sending highly sensitive information, such as your banking information or full credit card number. We also recommend that you use unique and strong passwords for your online account(s) and that you don’t share your passwords with anyone.

[30] The Claim incorporates by reference the Application and Agreement, thereby also incorporating by reference the Privacy Terms, Privacy Statement and Privacy Policy. For the purposes of the cause of action assessment under s. 4(1)(a) of the *CPA*, this means that I may consider inconsistencies between the facts in these

documents and facts pleaded in the Claim in determining whether a cause of action is disclosed: *Del Giudice* at paras. 43-48, 125-6; *Setoguchi v. Uber B.V.*, 2021 ABQB 18 at para. 63. I am satisfied that these documents are an integral part of the Claim. As such, the guidance of the Federal Court in *Jensen v. Samsung Electronics Co. Ltd*., 2021 FC 1185 at para. 86, is instructive:

> … it is appropriate for the certification judge to read the quotes and paraphrases contained in the pleadings in their context, by referring to their originating documents. If a plaintiff has ascribed a meaning to those paraphrases and quotes that is not consistent, on a plain reading, with the documents from which they originate, and if the documents referred to in the pleadings do not actually say what the Plaintiffs allege they say, the Court cannot consider these allegations as material facts, as they would not be true and would be incapable of proof. Indeed, counsel for the Plaintiffs conceded at the hearing before this Court that, if the allegations made in the Statement of Claim contain statements, paraphrases or facts that happen to be false or incorrect when compared to what the underlying documents actually contain, it is appropriate for the Court not to consider them or to give them no weight.

ANALYSIS

[31] Before turning to the test for certification, it is useful to address two issues. The first is the relevance of the *Del Giudice* decision here. The second is whether this action should include Québec in light of the current proceeding in Québec.

[32] In *Del Giudice*, Perell J. dismissed the plaintiff's application for certification of a national class action against Capital One arising out of the Data Breach, finding that none of the pleaded claims disclosed a cause of action under the Ontario equivalent of s. 4(1)(a). Capital One says *Del Guidice* is very persuasive because it arises out of precisely the same facts; Mr. Campbell says I should not accord it any special weight.

[33] The plaintiff's theory of the case in *Del Giudice* is broader and more complex than the claim before me, which is a relatively straight-forward data breach action. That is one of the reasons I granted carriage to Mr. Campbell: *Campbell* at para. 20. Perell J. discusses the complexity of the *Del Giudice* claim at length and it is an important reason why he denied certification: see, for instance, paras. 12-14, 268-270. Allowing for these differences, Perell J.'s consideration of those causes of

action that are also before me is helpful; that they arise out of the same facts contributes to their persuasiveness. I rely on *Del Giudice* to that extent.

[34] As I have noted, a class proceeding was commenced in Québec against Capital One on behalf of a Québec class in July 2019 ("Québec Action"). By virtue of the definition in s. 1 of the *CPA*, the Québec Action is a multijurisdictional proceeding for the purposes of the *CPA*, and s. 2(2)(b) required Mr. Campbell to give notice of this certification application to the Québec class.

[35] The parties to this application did not realize that notice had not been given until the certification hearing before me had commenced. I directed that notice be given and allowed class counsel in the Québec Action an opportunity to make submissions. Briefly, class counsel in the Québec Action oppose inclusion of a Québec class in this proceeding; Mr. Campbell maintains that there should be a single national class that includes Québec.

[36] The *CPA* addresses this issue in s. 4(3), which requires me to determine whether it is preferable for all or some of the claims or common issues to be decided in this action or in the Québec Action. Section 4(4) sets out what considerations guide that determination:

> (4) When making a determination under subsection (3), the court must
>
> (a) be guided by the following objectives:
>
> (i) to ensure that the interests of all parties in each of the relevant jurisdictions are given due consideration;
>
> (ii) to ensure that the ends of justice are served;
>
> (iii) to avoid irreconcilable judgments, if possible;
>
> (iv) to promote judicial economy, and
>
> (b) consider relevant factors, including the following:
>
> (i) the alleged basis of liability, including the applicable laws;
>
> (ii) the stage that each of the proceedings has reached;
>
> (iii) the plan for the proposed multi-jurisdictional class proceeding, including the viability of the plan and the capacity and resources for advancing the proceeding on behalf of the proposed class;

> (iv) the location of class members and representative plaintiffs in each of the proceedings, including the ability of representative plaintiffs to participate in the proceedings and to represent the interests of class members;
>
> (v) the location of evidence and witnesses.

[37] Class counsel in the Québec Action did not file any evidence in support of their position and no one provided me with the pleading in the Québec Action.[2] Based on the representations of counsel in their submissions, the relevant facts are:

- The Québec Action was filed before the Campbell Action was filed;
- The key facts underlying the two actions are the same (that is, the Data Breach);
- The Québec Action is based primarily on alleged breaches of the *CCQ*, Québec's privacy and consumer protection statutes, and the *Québec Charter of Human Rights and Freedoms*, R.S.Q., c. C-12;
- The Québec Action is being judicially case-managed by Justice Tremblay and several preliminary steps have been taken. A case management conference to set dates for an authorization hearing (equivalent to a certification hearing) is set for late March;
- About 100 Québec residents have registered on the website created by class counsel in the Campbell Action and the plaintiff says that registrants can access the site in multiple languages including French using "Google translate"; and
- Some 10,256 Québec residents have registered on the bilingual website created by Québec class counsel.

[2] Québec class counsel's concern that providing me with any evidence would constitute attornment to this jurisdiction is misconceived. The *CPA* expressly provides for participation by counsel from other jurisdictions at the certification stage without attornment.

[38] The key relevant factor in this case is s. 4(4)(b)(i). I say this because, although the authorization hearing has not occurred, the Québec Action is progressing. Essentially, it is one step behind this action. That is different from a situation where no steps have been taken in the other action. No one addressed the workplan. There is no material difference between these parties with respect to factors (iv) and (v).

[39] I accept that the Campbell Action and Québec Action assert the same or very similar bases of liability. The difference, in my view, lies in the way the two actions are likely to be pursued to promote the best interests of Québec residents.

[40] It is clear from the Claim and the submissions in the certification hearing that class counsel in the Campbell Action see the claims of Québec residents as analogous to the statutory claims of residents of common law jurisdictions and not particularly distinctive.

[41] For example, while Mr. Campbell stresses the importance of the breach of contract claim referring to articles of the *CCQ* relating to that claim and says it is not pleaded in the Québec Action, the Campbell Action does not actually plead breach of these articles. Under the heading “statutes”, para. 201 of the Claim states that the plaintiff pleads and relies on the *CPA*, *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5 [*PIPEDA*], negligence statutes, and consumer protection statutes. It does not mention the *CCQ*. As no one produced the claim in the Québec Action, I do not know whether it pleads breach of contract or not.

[42] By contrast, I understand that the whole focus of the Québec Action is on the liability of Capital One to Québec residents under Québec law.

[43] In the circumstances of this case, I consider that the interests of Québec residents and the ends of justice will be better served by excluding residents of Québec from the Campbell Action. In my view, the risk that the Québec Action will

not be certified is outweighed by the risk that the distinctive legal claims of Québec residents will not be fully addressed in the Campbell Action.

[44] There is little danger of irreconcilable judgments because the claims in the Québec Action are advanced under civil law. No one has suggested that there is a risk that interpreting Québec's consumer protection statute differently from another jurisdiction's consumer protection statute would lead to irreconcilable differences. I agree with Skolrood J.'s comment in *N&C Transportation Ltd. v. Navistar International Corporation*, 2021 BCSC 2046 at para. 50, that "there is considerable force to the submission of the defendants that litigating civil law and common law claims alongside one another in the same proceeding would add undue complexity to the matter."

[45] Therefore, I modify the class definition in this action to exclude residents of Québec.

[46] In closing on this issue, I want to be clear that I am not suggesting that multijurisdictional class actions in general should not include Québec. It will often be appropriate to do so to achieve the objectives in s. 4(4)(a) of the *CPA*. However, counsel seeking to certify a multijurisdictional class action including Québec must ensure that their pleading and submissions address the distinctive nature of Québec law. Equally, counsel opposing the inclusion of Québec must provide adequate evidence and submissions to the court hearing the issue that allow it to fully canvass the factors set out in s. 4(4).

Do the Pleadings Disclose a Cause of Action?

Negligence

[47] The four elements of a negligence claim are (1) the defendant owed the plaintiff a duty of care; (2) the defendant's conduct breached the standard of care; (3) the plaintiff suffered compensable damages; and (4) the defendant's breach caused the plaintiff's damages in fact and law: *1688782 Ontario Inc. v. Maple Leaf*

Foods Inc., 2020 SCC 35 at para. 18; *Mustapha v. Culligan of Canada Ltd.*, 2008 SCC 27 at para. 3.

[48] Capital One argues that Mr. Campbell has not adequately pleaded the existence of a duty of care, that he suffered compensable damages, or causation.

[49] Mr. Campbell acknowledges that he is asserting a novel duty of care and that he must satisfy the *Anns/Cooper* framework. He submits that the pleaded facts establish a sufficiently proximate relationship and foreseeability. The Claim defines the duty of care owed to the Class by Capital One as:

> …to keep their Personal Information confidential and secure, and to ensure that it would not be lost, disseminated or disclosed to unauthorized persons and to delete and destroy the Personal Information of applicants whose application[s] were rejected and customers whose credit cards were cancelled. …

[50] The plaintiff relies on *Tucci v. Peoples Trust Company,* 2017 BCSC 1525 [*Tucci* BCSC] rev'd in part 2020 BCCA 246 [*Tucci* BCCA]. There, Justice Masuhara found that it was not plain and obvious that a duty of care could not be found in a cyber-breach case because the pleaded facts were capable of establishing both a sufficiently close and direct relationship and reasonable foreseeability of harm:

> [123] In my view it is not plain and obvious that the first stage of the *Anns/Cooper* test is not met. The plaintiff has pleaded sufficient facts capable of establishing that harm was reasonably foreseeable. The information collected by Peoples Trust was sensitive and collected in the course of online applications for financial services. It is arguably reasonably foreseeable that harm such as identity theft could result if such information were disclosed or not securely stored, and it was again arguably foreseeable to Peoples Trust given the various policies and contractual terms it developed. Further, the plaintiff has pleaded sufficient facts that could establish a close and direct relationship between Peoples Trust and individuals who applied to it for financial services.

[51] The Court of Appeal agreed with this conclusion: at para. 51.

[52] The Claim pleads the following damages:

> Upon being notified of the Breach, Class Members have experienced fear and apprehension, anxiety, anger, risk, confusion and humiliation in relation to the unauthorized or unknown future use of their Personal Information. To mitigate the risks, Class Members have taken all reasonable steps necessary

> to protect their credit reputation and secure their finances including hours of wasted time, lost income and inconvenience involved in applying for and the cost of credit monitoring services and identity protection services, monitoring credit reports issued by credit reporting services, placing credit flag/fraud alerts with credit reporting companies, prolonged credit transactions due to the credit flags, changing passwords, notifying financial institutions and applying for a new social insurance number from Service Canada.

[53] Put succinctly, the pleaded damages consist of (1) emotional distress, (2) increased risk of harm, and (3) the costs of mitigating against that risk.

[54] While the first two types of loss may not be compensable absent pleading actual loss, expenses actually incurred to mitigate against the risk of future loss are compensable damages and satisfy the third element of a negligence claim. In *Obodo v. Trans Union of Canada, Inc.*, 2021 ONSC 7297, which was also a data breach case, the court rejected the same objection that Capital One advances here. After considering the relevant authorities, Glustein J. concluded that it was not settled law that the claims for out of pocket damages and mental distress cannot constitute damages in a class action and held that the claim before him disclosed a cause of action in negligence: at para. 160; see also *Kaplan v. Casino Rama*, 2019 ONSC 2025 at para. 22.

[55] Capital One relies on *Babstock*. There, at para. 27, Brown J. for the majority held that disgorgement is a remedy, not an independent cause of action. That means that a plaintiff must prove all elements of negligence, including actual damages, before it can seek disgorgement: at paras. 32-33. The plaintiffs in *Babstock* did not plead the loss element of negligence. By contrast, Mr. Campbell has pleaded loss arising from the costs of risk mitigation.

[56] Even where there is a viable negligence claim, disgorgement may not be available. In *The Insurance Corporation of British Columbia v. Teck Metals Inc*., 2022 BCSC 374, Justice Riley struck a claim for disgorgement as disclosing no reasonable cause of action where the alleged negligence arose from acid spills on a highway. He noted (at para. 19) that Justice Branch had allowed a disgorgement claim arising out of alleged negligence in the contents of health supplement products in *Krishnan v. Jamieson Laboratories Inc.*, 2021 BCSC 1396.

[57] Riley J. found that that a disgorgement remedy was not available where losses are quantifiable:

> [22] As noted, disgorgement is an exceptional remedy only available where traditional remedies would not provide an adequate legal response to the actionable wrongful conduct of the defendant. Traditional remedies may be inadequate where, for example, the plaintiff's loss is impossible to calculate, or where the plaintiff's interest in the defendant's performance of its legal obligations is not reflected by a purely economic measure: *Atlantic Lottery* at para. 59.
>
> [23] In the case at bar, the plaintiff's second amended notice of civil claim seeks damages as compensation for various amounts of money paid out or expended internally in connection with the acid spills that are the subject of the action. These damages include: (i) compensation for amounts paid out to insureds whose vehicles were determined to be exposed to acid from the spills; (ii) costs for towing of vehicles that had to be inspected, together with costs for replacement vehicle rentals for those owners; and (iii) costs of investigating the claims arising from the acid spills. Thus, the plaintiff is clearly able to identify various categories of loss it has suffered in connection with the acid spills, and to place a monetary value on each category of loss.
>
> [24] The plaintiff's claim for disgorgement of profits is framed as a supplementary or alternative form of relief. The plaintiff does not allege that more conventional forms of damage would be inadequate for any reason.
>
> [25] On the basis of the pleadings, there is no suggestion that the plaintiff's losses would be impossible to calculate. Indeed, the alleged losses are reflective of monies paid out or expenses incurred by the plaintiff, by way of insurance payments to individual insureds, towing and replacement vehicle rental costs, and costs of investigating the vehicle damage claims.

[58] Here, the pleaded losses are also routinely pleaded and quantified in negligence actions. They include out of pocket expenditures and time spent to protect against he risks of misuse of Confidential Information. The pleading does not contain material facts showing that the plaintiff has a legitimate interest in Capital One’s profits. I conclude that the pleadings disclose a cause of action in negligence, but do not disclose a disgorgement remedy.

[59] Before leaving this issue, I note that the plaintiff pleads joint and several liability under s. 4(2)(a) of the *Negligence Act*, R.S.B.C. 1996, c. 333, and equivalent provisions in other common law provinces. That subsection does not create a cause of action. It addresses allocation of liability by stipulating that where two or more persons are at fault for a loss, they are jointly and severally liable. The loss must be global or indivisible: *WorleyParsons Canada Ltd. v. David Nairn and Associates*,

2013 BCCA 513 at para. 19. Mr. Campbell has pleaded that Capital One and Ms. Thompson engaged in tortious conduct and that the plaintiff's loss is indivisible. That is sufficient to engage the statute for certification purposes.

Breach of Contract

[60] The Claim pleads that, in addition to the Agreement, there was also a contract between Capital One and those who applied for credit cards but whose Applications were rejected. Capital One says the application form was not a contract. It also takes issue with the plaintiff's position on which Capital One entities were the contracting parties.

Was the Application a Contract?

[61] The Application expressly states that it is an offer by the applicant to enter into a contractual relationship with Capital One:

> Terms of Offer
>
> By submitting the Application Form, the applicant ("I"):
>
> 1. Certify that the information provided is true and correct and understand that Capital One Bank (Canada Branch), ("Capital One"), will rely on this and other information in deciding to open a MasterCard Account ("Account");
>
> 2. Request that Capital One open an Account and issue appropriate MasterCard card(s) ("Card(s)") and Personal Identification Number(s) to me (including renewals and replacements from time to time);
>
> 3. Request that Capital One issue appropriate Cards to me for any Authorized User identified on the Application Form, as well as renewals and replacements from time to time;
>
> 4. Agree that use of the Account or Card(s) will confirm acceptance of Capital One's MasterCard Customer Agreement as amended from time to time (the "Agreement"), which will be sent with my Card(s) if approved; …

[62] The Claim characterizes this language as a contract, "formed when the applicant provided Capital One with Personal Information in exchange for consideration of the applicant's application for a credit card." On its face, that is an untenable interpretation of unambiguous contractual language. It is plain and obvious that the claim based on the existence of a contract between unsuccessful credit card applicants and Capital One is bound to fail.

Who are the parties to the Agreement?

[63] Current and former cardholders are parties to the Agreement. The Claim pleads that both Capital One (Canada Branch) and Capital One Financial Corporation are parties to the contract and, in the alternative:

> … Capital One Canada entered into the contract(s) on behalf of and with the ostensible authority of Capital One, who established Capital One Canada to be its authorized agent in Canada. Through the use of its trademark and logo in the contract(s) and assurances it made in the Privacy Statement section of the contract(s), Capital One intended to convey to customers and did convey that its agent in Canada, Capital One Canada had ostensible authority to enter into the contracts on its behalf. Therefore, Capital One in its capacity as principal is liable, together with Capital OneCanada for breaches of the contract.

[64] Capital One says that the contract is only between Capital One (Canada Branch) and the current or former cardholder.

[65] The Agreement expressly defines the contracting parties:

> In this Agreement, the words "you," "your" and "yours" refer to the applicant and any co-applicant who, according to our records, was identified as such as part of the application, meaning the request to us for the account. These words do not include an authorized user. The words "we," "us" and "our" mean the Capital One® Bank (Canada Branch) and its successors or assigns.

[66] Mr. Campbell points to the "Capital One" trademark that appears on the cover page of the Agreement. The last page of the Agreement states that Capital One is a registered trademark and "All trademarks used herein are owned by their respective entities." The trademark also appears on the Application where, in very small print, it is stated to be the trademark "of Capital One Financial Corporation used under licence."

[67] Capital One submits that there is no authority for the proposition that the presence of a trademark on a document makes the holder of a trademark a contracting party, noting that the ubiquitous presence of manufacturer trademarks on goods sold by retailers does not mean that manufacturers are thereby contracting with consumers. I agree. The Agreement defines the contracting parties as Capital

One (Canada Branch) and the cardholder. The Claim does not disclose a cause of action for breach of contract against Capital One Financial Corporation.

Is there a Cause of Action in Contract against Capital One (Canada Branch)?

[68] The Agreement is a contract of adhesion and this fact informs consideration of the breach of contract claim. Specifically, any ambiguity should be interpreted in favour of the plaintiff: *Zurich Life Insurance Co. of Canada v. Davies*, [1981] 2 S.C.R. 670 at 674.

[69] Before determining whether the Claim discloses a cause of action for breach of contract, I must consider whether it is possible to interpret the Agreement as incorporating by reference the requirements of *PIPEDA*. If it does, the breach of contract claim would include breach of *PIPEDA*. For example, the Claim pleads that Capital One's failure to delete and destroy the personal information of former cardholders when they ceased to be cardholders. The source of this requirement is *PIPEDA*.

[70] The Claim pleads that "[b]y promising to comply with applicable privacy legislation in its Privacy Policy, Capital One incorporated applicable privacy legislation into the contract, including *PIPEDA.*"

[71] However, the only explicit reference to *PIPEDA* is in section 1 of the Privacy Policy:

> 1. PRIVACY COMMITMENT AND PERSONAL INFORMATION
>
> Capital One® is committed to keeping personal information accurate, confidential and secure.
>
> We collect, use and disclose personal information to operate our business and as required by law. Personal information is information about an identifiable individual, as defined in the Personal Information Protection and Electronic Documents Act.

[72] There are three other references to “laws” in the Privacy Policy:

> 5. CONSENT
>
> If you apply for a credit product, communicate with us or provide personal information to us in any way, you acknowledge your consent for personal information collection, use and disclosure as set out in this Policy or applicable laws and industry standards.
>
> 6. LIMITING COLLECTION
>
> Capital One only collects personal information that’s necessary for the purposes we identify, and as required by applicable laws.
>
> 7. LIMITING USE, DISCLOSURE AND RETENTION
>
> Capital One limits use, disclosure and retention of personal information to the purposes we identify, and as required by applicable laws.

[73] It is open to contracting parties to choose to incorporate legislative requirements into their contracts. The question is whether, in light of the contractual language, there is any air of reality to the plaintiff’s claim that *PIPEDA* is incorporated into the Agreement.

[74] Even reading the Claim as generously as possible, the Privacy Policy does not commit Capital One to compliance with *PIPEDA*, thereby incorporating *PIPEDA* into the terms of the Agreement. The language of the Agreement is not ambiguous. It expressly incorporates only *PIPEDA’s* definition of personal information.

[75] The three references to “other applicable laws” do not specify what those laws are either in those clauses or anywhere else in the Agreement. The passage under the heading “consent” explains that the individual is consenting to Capital One’s collection, use, and disclosure of personal information as explained in its policy, or applicable laws or industry standards. This passage does not say or imply that Capital One will not collect, use, disclose or retain personal information unless authorized to do so under *PIPEDA*. The references to “applicable laws” under the headings “Limiting Collection” and “Limiting Use, Disclosure and Retention” say that that any constraints on collection, use, disclosure and retention are those set out by Capital One and applicable laws. These passages do not say or imply that Capital One’s purposes for collection, use, disclosure or retention are restricted to purposes authorized by *PIPEDA*.

[76] The cases on which the plaintiff relies are distinguishable because in each the court found that the contractual language was ambiguous and could reasonably be interpreted as incorporating a particular law. In *Sharp v. Royal Mutual Funds Inc*., 2020 BCSC 1781 at para. 97 aff'd 2021 BCCA 307, there was a live question as to whether the relevant contract's references to Canadian securities legislation was purely informational, or intended to actually confer rights. The language of the Agreement in this case does not give rise to any similar questions. See also *Berenguer v. SATA Internacional – Azores Airlines, S.A.*, 2021 FC 394 at para. 84.

[77] Further, the Agreement expressly authorizes Capital One to collect, use, disclose and retain personal information in ways prohibited by *PIPEDA*. For example, the Agreement does not prohibit Capital One from retaining the personal information of former cardholders, whereas *PIPEDA* does.

[78] I conclude that it is plain and obvious that the portion of the breach of contract claim based on a breach of *PIPEDA* is bound to fail.

[79] However, the breach of contract claim does not rest exclusively on *PIPEDA*. The Claim also pleads that Capital One breached the Agreement by failing to employ sufficiently strict safeguards against unauthorized access and failing to encrypt user data. It sets out the following particulars:

- they failed to hire competent employees, they failed to properly supervise their employees, or they failed to provide proper training to their employees;
- they failed to encrypt the data, storing it in 'plain-text' instead;
- they failed to filter traffic from suspicious IP addresses or to catch the transfer of 28 GB of data out of their servers to the suspicious IP addresses;
- they failed to properly limit the access granted to the account used by the Hacker to the access necessary for the account's role or have processes to monitor when it was being used for a process it was not needed for;
- they failed to implement adequate security monitoring procedures resulting in the defendants failing to detect the breach for several months. At the time of pleading the defendants would be unaware of the breach had it not been for a tip from a white hat cyber source.

[80] The Claim pleads compensatory and nominal damages and seeks disgorgement. For the reasons set out above in relation to the negligence claim, I find that compensatory damages are adequately pleaded. A plaintiff may disclaim compensatory damages in favour of nominal damages: *Sharp* at para. 164.

[81] With respect to disgorgement, the Supreme Court of Canada has established that disgorgement may be available for breach of contract in "certain exceptional circumstances", and only where damages, specific performance and injunction are inadequate and the circumstances warrant. An important consideration is whether the plaintiff had a legitimate interest in preventing the defendants' profit-making activity: *Babstock* at paras. 53, 59.

[82] In *Babstock* at para. 60, Justice Brown states that, "compensatory damages are not inadequate merely because a plaintiff is unwilling, or does not have sufficient evidence, to prove loss". Rather, the inadequacy must flow from the nature of the plaintiff's interest. Justice Brown found that there was nothing exceptional about a breach of contract arising from allegedly deceptive video lottery terminals that could give the class of plaintiffs in that case a legitimate interest in the defendant's profit-making activity.

[83] Here, the Claim pleads that the plaintiffs' "contract interest is such that it cannot be vindicated by other forms of contractual relief and cannot possibly be quantified in monetary terms". The Claim refers to the need to "deter the wrongdoer", the "trust, confidence and vulnerability" of class members, and the importance of privacy interests. Notably absent are material facts that are capable of establishing that the class has any legitimate interest in Capital One's profit-making activity. As counsel put it, albeit in another context, "this is a straightforward data breach case". It is plain and obvious that a claim for disgorgement damages for breach of contract cannot succeed.

[84] Subject to these limitations, the breach of contract claim is adequately pleaded.

Breach of Express and Implied Warranties

[85] The Claim pleads breach of warranties as follows:

> 59. Through its Customer Agreement, Privacy Statement and Privacy Policy, the defendants continually warranted to customers that it took their privacy seriously and that protecting their Personal Information was a paramount concern and that it would keep their Information private and confidential with an intention to prevent identity theft. Further, the defendants warranted or guaranteed "The personal information you share with us, stays with us".
>
> 60. The defendants breached its warranties by not taking customer privacy seriously, by not making customer Personal Information its paramount concern, and by not guaranteeing the Personal Information shared with Capital One stayed with Capital One.

[86] I agree with Capital One that the Agreement does not warrant that Capital One will not disclose customer personal information to others. In fact, it expressly states that it will disclose such information to third parties for stated purposes. The Agreement does not represent that protection of such information is Capital One's "paramount" concern or that its data storage system is impenetrable. Taking privacy "seriously" is the kind of subjective description that does not give rise to enforceable contractual obligations: *First City Dev. Corp. v. Bekei* (1986), 3 B.C.L.R. 175 at 208-209 (S.C.); *Topnotch Developments Ltd. v. Welldone Ventures Canada Inc.*, 1991 CanLII 596 (B.C.S.C.). The breach of warranty claims are bound to fail.

Breach of Contractual Duty of Honest Performance

[87] As the Supreme Court of Canada held in *C.M. Callow Inc. v. Zollinger*, 2020 SCC 45 at para. 81 [*Callow*], this cause of action arises only where a defendant engages in active dishonesty or deception that is directly related to the performance of the contract. Put another way, the central element is whether one contracting party lied or knowingly misled the other: *Callow* at para. 88.

[88] The Claim does not contain this element. Mr. Campbell pleads that the statements made in the Agreement about the security measures in place to protect the Confidential Data amounted to a promise that there would be no unauthorised access to it.

[89] However, nothing in the Agreement can be read as representing anything more than that Capital One has implemented security measures to protect against hacking. For example, the Privacy Statement says:

> Capital One® is committed to keeping your personal information accurate, confidential and secure. We want to earn your trust by providing strict safeguards to protect your information.

[90] The Privacy Policy states:

> Capital One uses procedures and practices appropriate to the sensitivity of personal information to protect against loss, theft and unauthorized access. Access to your information is restricted to those individuals and parties who require access.
>
> For example, we have physical security (such as restricted access to our offices and secure storage), electronic protection (such as passwords and encryption) and safe business practices (such as customer authentication when you call us). We also train our staff on how to safeguard personal information.

[91] The Claim does not plead that Capital One lied to or knowingly misled cardholders about the security measures it had implemented. It pleads that the measures were inadequate, based on the fact that the Data Breach occurred. As such, the Claim does not plead material facts that amount to the kind of active deception or dishonesty necessary to prove breach of the contractual duty of honest performance. In other data breach cases, courts have refused to certify breach of confidence claims based on an argument that inadequate security measures after a hacking event amounts to "misuse" of the confidential information by the defendant: *Tucci* at paras. 140-141; *Kaplan* at paras. 31-32. I consider the claim of breach of contractual duty of honest performance analogous to those cases.

[92] It is plain and obvious that this cause of action is bound to fail.

Breach of Confidence

[93] The elements of a breach of confidence claim are (1) the information was confidential; (2) it was communicated in confidence; and (3) it was misused by the party receiving it: *Lac Minerals Ltd. v. International Corona Resources Ltd.*, [1989] 2 S.C.R. 574 at 608.

[94] The Claim does not plead that the Data Breach or the security measures that failed to prevent it were a misuse of the confidential information by Capital One, possibly because that argument was rejected in *Tucci* BCCA at paras. 113-114; see also *Kaplan* at para. 31. Instead, Mr. Campbell pleads that Capital One misused the confidential information by retaining it after it should have been deleted. As counsel acknowledged in oral submissions, this argument rests on finding that the Agreement incorporates *PIPEDA*. It also rests on a conclusion that *PIPEDA*'s requirements prevail over the express terms of the Agreement, which say that Capital One may retain, use and disclose the Confidential Data of unsuccessful applicants and former customers.

[95] As I have found that the Agreement does not incorporate *PIPEDA* by reference, it is plain and obvious that the breach of confidence claim is bound to fail.

Intrusion Upon Seclusion

[96] The tort of intrusion upon seclusion is recognized in some but not all jurisdictions. Its status is unclear in data breach cases like this where the defendant is alleged to have "intruded" by failing to prevent an independent third party from hacking into a database.

[97] In *Tucci* BCSC, Masuhara J. concluded that the tort does not exist in the context of a data breach case. However, Mr. Campbell invites me to find that it does on the basis of the Court of Appeal's comments in *Tucci* BCCA. There, Justice Groberman characterized the failure to appeal that aspect of the certification judge's ruling as unfortunate and suggested that "the time may well have come for this Court to revisit its jurisprudence on the tort of breach of privacy": at para 55. He added (at para. 66):

> It may be that in a bygone era, a legal claim to privacy could be seen as an unnecessary concession to those who were reclusive or overly sensitive to publicity, though I doubt that that was ever an accurate reflection of reality. Today, personal data has assumed a critical role in people's lives, and a failure to recognize at least some limited tort of breach of privacy may be seen by some to be anachronistic.

[98] Justice Groberman is, of course, referring to the timing of the Court of Appeal's reconsideration of the issue, not to reconsideration by this court. The Court of Appeal could revisit the question of recognizing a breach of privacy tort in an appeal from a decision declining to recognize the tort just as much as it could in a case where it was found to exist.

[99] Nothing in the Court of Appeal's reasons suggests that I ought to disregard the longstanding principle of judicial comity in *Re Hansard Spruce Mills Ltd.,* [1954] 4 D.L.R. 590 (B.C.S.C.).

[100] Privacy breach cases, including class action data breach cases, are coming before the courts with increasing frequency. Considering the present uncertainty in Ontario law as to whether a defendant commits the tort where a third party hacks its database, as I discuss below, the plaintiff has not convinced me to go against Masuhara J.'s ruling in *Tucci* BCSC.

[101] Although the decision in *Jones v. Tsige*, 2012 ONCA 32, in Ontario is often cited as the basis for recognizing the intrusion tort, in that case, the defendant committed the intrusive act by accessing the plaintiff's bank account herself.

[102] More recently, Ontario certification cases have held that a defendant who is the custodian of a database does not commit this tort by failing to prevent an independent third party from hacking into the database. In *Owsianik v. Equifax Canada Co.*, 2021 ONSC 4112, the majority of the Divisional Court held that the tort of intrusion upon seclusion could not apply to find a database defendant liable for hacker attacks. Justice Ramsay wrote:

> [54] The tort of intrusion upon seclusion was defined authoritatively only nine years ago. It has nothing to do with a database defendant. It need not even involve databases. It has to do with humiliation and emotional harm suffered by a personal intrusion into private affairs, for which there is no other remedy because the loss cannot be readily quantified in monetary terms. I agree that Sharpe J.A.'s definition of the tort is not necessarily the last word, but to extend liability to a person who does not intrude, but who fails to prevent the intrusion of another, in the face of Sharpe J.A.'s advertence to the danger of opening the floodgates, would, in my view, be more than an incremental change in the common law.

> [55] I agree with my colleague (paragraph 43) that Equifax's actions, if proven, amount to conduct that a reasonable person could find to be highly offensive. But no one says that Equifax intruded, and that is the central element of the tort. The intrusion need not be intentional; it can be reckless. But it still has to be an intrusion. It is the intrusion that has to be intentional or reckless and the intrusion that has to be highly offensive. Otherwise the tort assigns liability for a completely different category of conduct, a category that is adequately controlled by the tort of negligence.
>
> [56] For that reason I respectfully disagree with the decision in *Kaplan v. Casino Rama*, 2019 ONSC 2025 and the motion judge's decision in *Tucci v. Peoples Trust Company*, 2017 BCSC 1525. I distinguish *Bennett v. Lenovo*, 2017 ONSC 1082 on the basis that the manufacturer was said to have intruded by installing adware (a kind of spyware) on the computers that it sold to the public.
>
> [57] The plaintiffs here are not without remedy. The essence of their claim has to do with risk to economic interests caused by disclosure of their financial information. It is not too much to ask that they prove their damages. See *Babstock*, paragraph 60. The tort of negligence protects them adequately and has the advantage that it does not require them to prove recklessness.

See also *Obodo* at para. 22; *Del Giudice* at paras. 135-147; *Winder v. Marriott International, Inc.*, 2022 ONSC 390 at paras. 13-18; *Stewart v. Demme*, 2022 ONSC 1790.

[103] The Ontario Court of Appeal has granted leave to appeal in *Owsianik* and the hearing is scheduled for June 2022. The outcome of that appeal may change the current law in Ontario and may be persuasive if the Court of Appeal decides to revisit the issue in British Columbia. Just as the fact that a claim is novel is not itself sufficient reason to certify it (*Babstock* at para. 19), the possibility that the law may change is an insufficient basis for certification.

[104] It is plain and obvious that this cause of action is bound to fail.

Statutory Privacy Torts

[105] The plaintiff alleges breaches of the BC *Privacy Act*, R.S.B.C. 1996, c. 373, and of similar statutes in Saskatchewan, Manitoba and Newfoundland and Labrador.

[106] Capital One argues that I do not have jurisdiction to adjudicate claims under the Manitoba and Newfoundland and Labrador privacy statutes because, like the BC

Privacy Act, each of these statutes expressly confers jurisdiction on certain courts of that province.

[107] For the reasons set out in *Douez v. Facebook Inc.* 2022 BCSC 914, I have jurisdiction to adjudicate claims arising from the Manitoba and Newfoundland statutes. As Capital One has not argued *forum non conveniens*, I may not decline to exercise jurisdiction: *Club Resorts Ltd. v. Van Breda*, 2012 SCC 17 at para. 102.

[108] Manitoba's privacy statute does not require a plaintiff to prove the violation was wilful. Subsection 2(1) of *The Privacy Act*, C.C.S.M. c. P125, provides that "[a] person who substantially, unreasonably, and without claim of right, violates the privacy of another person, commits a tort against that other person."

[109] The three other pleaded privacy statutes require the party asserting breach of privacy to prove that the defendant "wilfully" invaded their privacy: *Privacy Act*, s. 1(1); *Privacy Act*, R.S.N.L. 1990, c. P-22, s. 3(1); *The Privacy Act*, R.S.S. 1978, c. P-24, s. 2. The plaintiff must prove that the defendant intended to violate the plaintiffs' privacy; it is not enough to show that the defendant engaged in an intentional act that is causally related to an unintentional intrusion: *Cole v. Prairie Centre Credit Union Ltd.*, 2007 SKQB 330 at paras. 40-46; *Del Giudice* at para. 164. The latter is a claim in negligence, which I have already discussed. In *Del Giudice* at para. 163, Perrell J. found that the plaintiff's statutory tort claims against Capital One were bound to fail because, "it is not wilfulness to fail to prevent a third party from invading another's privacy"

[110] In *Hollinsworth v. BCTV*, 59 B.C.L.R. (3d) 121 at para. 29 (C.A.), the Court considered that "wilfully" may include an objective element when it referred to "an intention to do an act which the person doing the act knew or should have known would violate the privacy of another person." In *Duncan v. Lessing*, 2018 BCCA 9, the Court of Appeal noted that the inclusion of an objective element in the definition of wilfulness was out of step with how the word, when used in a statutory context, is most frequently defined; however, the Court declined to revisit the definition: at para. 86; see also *Agnew-Americano v. Equifax Canada Co.*, 2019 ONSC 7110 at

para. 238. Thus *Duncan* establishes that wilful conduct cannot be accidental but does not say whether or not recklessness can constitute wilfulness for the purposes of the BC statute.

[111] In *Kumar v. Korpan*, 2020 SKQB 256, the Saskatchewan Queen's Bench found that recklessness will not constitute wilfulness under that province's privacy act, but also commented (at para 36) that, "there is no firm agreement across the country as to what 'willfully' entails in the context of privacy legislation".

[112] In *Obodo*, Glustein J. would have certified the statutory privacy tort claims in Saskatchewan, Newfoundland and Labrador, and BC on the basis that (at para. 215):

> …it is not settled law that a database defendant could not be found to have engaged in a wilful breach of privacy under the provincial privacy legislation if the plaintiff alleges that the conduct was 'intentional' or 'wilful' (which could include reckless conduct), which the database defendant knew or should have known would violate the privacy of another person."

[113] I agree: absent a definitive appellate ruling on whether wilfulness includes recklessness, it is not plain and obvious that the pleaded conduct of the defendant was not wilful.

Breach of Consumer Protection Legislation

[114] The Claim pleads breach of the consumer protection laws of each jurisdiction. Consumer protection legislation must be interpreted generously in favour of the consumer it is intended to protect: *Seidel v. TELUS Communications Inc.*, 2011 SCC 15 at para. 37.

[115] An essential element of each of these causes of action is that the defendant made misleading representations: *Krishnan* at para. 74. That means the plaintiff must have pleaded material facts that, if true, are capable of being found to be misleading representations. Capital One argues that Mr. Campbell has not done so.

[116] The Claim identifies the following representations in the Agreement as misleading:[3]

a) "Capital One is committed to keeping your personal information accurate, confidential and secure. We want to earn your trust by providing strict safeguards to protect your information."

b) "We respect your privacy. Not only do we respect it, but we also protect it. The personal information you share with us stays with us."

c) "We restrict access to your personal information to those who need to have it to provide products or services to you. We select [those companies] carefully and require them to keep the information we share with them safe and secure. We do not allow them to use or share information for any purpose other than the job they are hired to do. They must meet our rigorous safety standards before we partner with them."

d) "We use procedures and practices appropriate to the sensitivity of personal information to protect against loss, theft, and unauthorized access. Access to your information is restricted to those individuals and parties who require access."

e) "We comply with applicable laws."

f) "We have physical security (access in buildings), electronic protection (encryption), and safe business practices (customer authentication when you call us) to prevent identity theft. We also train our staff on how to safeguard personal information."

[117] I agree with Capital One that the fact that the Data Breach occurred does not make the first five of these representations untrue. The situation is analogous to

[3] I have set out those representations relevant to the Data Breach and eliminated duplication. The Privacy Terms, Privacy Statement and Privacy Policy are reproduced more fully at paragraphs 20-29 above.

Evans v. General Motors of Canada Company, 2019 SKQB 98, where the court found that a defect in a car that was represented as safe and reliable was not misleading: at para 62; see also *Williams v Canon Canada Inc*., 2011 ONSC 6571 para. 227. As discussed in these cases, general promotional statements about the quality of a product or device are not factually specific enough to be capable of being false or misleading.

[118] The plaintiff has no cause of action under consumer protection laws in respect of general promotional statements. However, the sixth pleaded misrepresentation arguably goes beyond general promotion. While the fact of the Data Breach does not make this representation misleading, the representations in this passage are factual, and the Claim pleads material facts that they are false. It pleads that Capital One failed to designate individuals responsible for network security management of personal information, stored personal information on an unsecured network and server, and failed to encrypt personal information.

[119] Assuming the truth of these facts, it is not plain and obvious that a breach of consumer protection law claim is bound to fail.

[120] I agree with Capital One that, in the circumstances of this case, there is no "duty to warn" for the reasons discussed above under duty of contractual honesty, and that there is no consumer protection cause of action for failing to secure personal information.

[121] With respect to damages, I have found that the plaintiff has pleaded compensable loss. If successful, the class would be entitled to provable losses.

[122] I conclude that there is a cause of action for breach of consumer protection laws, albeit in a more circumscribed form than that pleaded.

CONCLUSION ON CAUSES OF ACTION

[123] In conclusion, the Claim discloses causes of action in negligence, contract, and breach of consumer protection laws, although they are narrower than framed in

the Claim. The causes of action in breach of warranty, breach of the duty of honest performance, breach of confidence, and intrusion upon seclusion are bound to fail. It is also plain and obvious that disgorgement is not available as a remedy for the pleaded negligence.

[124] In the following section I will address whether the plaintiff has provided some basis in fact that the causes of action disclosed by the Claim satisfy the requirements in ss. 4(1)(b)-(e) of the *CPA*.

SOME BASIS IN FACT

Some Basis in Fact for Compensable Loss in Data Breach Cases

[125] Capital One submits that there is no basis in fact that the Claim satisfies any of the requirements in ss. 4(1)(b) to (e) because there is no admissible evidence that any of the proposed class members have suffered any compensable loss. Capital One argues that, absent any evidence that the Confidential Information was actually disseminated, the proposed class members cannot have suffered any loss. It also challenges the admissibility of the evidence of what out-of-pocket expenses, such as credit monitoring and identity theft protection, proposed class members incurred.

[126] Courts have accepted that a demonstrated real risk of future harm may give rise to compensable loss even where there is no evidence that stolen data has been used: *Tucci* BCSC at paras. 200-201; *Obodo* at para. 137.[4] In *Kaplan* at paras. 21-22, the Court noted that losses such as damage to credit reputation, costs of credit monitoring, and costs incurred in preventing or rectifying identity theft are compensable in breach of privacy class actions. As I read these authorities, the question of whether victims of a data breach have suffered compensable loss because of the risk that the stolen information will be disseminated in a manner damaging to them requires the plaintiff to show, on the “some basis in fact” standard:

[4] In *Setoguchi*, certification was denied because the court found that the evidence demonstrated some basis in fact that there was *no* actual harm or loss. Thus, the loss was purely speculative.

a) that there is a real risk, not merely a subjective fear, of future loss due to the data breach;

b) that the defendant has not provided mitigation measures adequate to protect against that risk; and

c) that the plaintiff incurred out-of-pocket costs to protect against that risk.

[127] If so, the court will consider whether the plaintiff has established some basis in fact for the criteria in ss. 4(1)(b) to (e).

[128] Courts have repeatedly emphasized that the “some basis in fact” inquiry is case specific. While reviewing other cases may illustrate the application of general principles, evidentiary assessments turn on the evidence and issues before the court: *Harris v. Bayerische Motoren Werke Aktiengesellschaft*, 2019 ONSC 5967 para. 50. It is also important to remember that the focus at the certification stage is on whether a class proceeding is the appropriate form of action. Beyond the low “some basis in fact” threshold, there is no analysis of the substantive merits of the claim: *Hollick v. Toronto (City)*, 2001 SCC 68 at para. 16; *Finkel v. Coast Capital Savings Credit Union*, 2017 BCCA 361 at para. 19.

[129] In this case, Dr. Scheurkogel’s evidence provides some basis in fact that there is a real risk that the Confidential Information will be used in ways harmful to the Class. Dr. Scheurkogel is a cyber-security expert. He agrees that there are no indications to date that the Confidential Information has been used or disseminated. However, he deposes that it is possible, in light of the length of time between the Data Breach and Ms. Thompson’s arrest, her intention to profit from it, and the sophistication of the theft, that Ms. Thompson has secreted the Confidential Information somewhere for future dissemination. He says that social insurance numbers have lasting value on the black market as they tend not to change, and that criminal groups may wait before using “hot” information. Dr. Scheurkogel points out that Capital One has not disclosed what, if any, searches it has conducted on the dark web for indications the Confidential Information has been used.

[130] The fact that Capital One offered such protection, in the form of two years of free credit monitoring and identity theft protection by TransUnion, also supports a conclusion that the risk was real and reasonable for some period of time.

[131] Capital One argues that the risk mitigation protection it offered fully addressed the risk attributable to the Data Breach, relying on *Maginnis v. FCA Canada Inc*., 2021 ONSC 3897. That was a certification application for a class action arising from defective eco-diesel car engines built by the defendant. The defendant had recalled and repaired the defective vehicles. The Divisional Court concluded that it was open to the judge to find that the repair adequately compensated the plaintiffs for their loss:

> [48] Ultimately, the motion judge determined that the remedy provided by the repair FCA offered was a remedy that provided access to justice for class members. He did so as he had found there was no evidence of any compensable loss remaining after the repair, and nominal damages were not enough to justify certification. He also concluded that the behaviour modification objective was met. Finally, he considered that a class proceeding would not be a wise use of judicial resources in this case. His finding is consistent with the Supreme Court's decision in *Atlantic Lottery.*

[132] Unlike the defendant in *Maginnis*, there is evidence here that Capital One did not fully "repair" the problem. Dr. Scheurkogel describes two limitations of the risk mitigation measures offered by Capital One. First, it is temporary: the free credit monitoring and identity theft protection offered through TransUnion expires after two years. Second, coverage is partial: some major banks, such as TD Bank, CIBC, Desjardins and HSBC, do not report to TransUnion.

[133] In his third affidavit, Mr. Campbell deposes that he purchased credit monitoring with Equifax for $20.95 per month because of his concerns about identity theft. Equifax receives reports from banks that do not report to TransUnion. In his first affidavit, Mr. Campbell attributes those concerns to the Data Breach.[5] This

[5] While Capital One tendered evidence that Mr. Campbell may have been the victim of other data breaches in 2018 and 2019, this does not detract from his evidence that he purchased the Equifax product because of the Capital One Data breach for the purposes of the "some basis in fact" assessment.

evidence satisfies the plaintiff's obligation to demonstrate some basis in fact that Capital One has not provided adequate risk mitigation measures.

[134] I conclude that the plaintiff has established some basis in fact for compensable loss.

Some Basis in Fact - Identifiable Class

[135] A representative plaintiff must define a class with reference to objective criteria, independent of the merits of the claim, that is rationally related to the common issues such that it is clear who is entitled to notice, who is entitled to relief and who is bound by any judgment. The evidence must provide some basis in fact that at least two persons could self-identify as class members and later prove that they are members of the class: *Finkel* at para. 21, citing *Jiang v. Peoples Trust Company*, 2017 BCCA 119 at para. 82.

[136] Mr. Campbell's proposed class definition is:

> All Canadians who applied for or were issued a Capital One credit card and who were notified by the defendants that their information may have been compromised in the Breach.

[137] The Claim defines "Breach" as a cybersecurity breach of a Capital One database between March 12 and April 21, 2019.

[138] As I have excluded Québec residents, the class definition must be amended to read "All Canadians except for residents of the Province of Québec".

[139] This Class definition is based on objective and easily ascertainable criteria. Capital One does not argue otherwise. I am satisfied that Mr. Campbell has shown some basis in fact that the risk of dissemination has caused compensable loss.

[140] The real issue under this heading is whether the plaintiff has established that at least two persons could self-identify as class members and later prove that they are members of the class.

[141] There is no affidavit evidence from another potential class member. Instead, the plaintiff tendered evidence of an expert's analysis of the information provided by people who chose to register on the website created by class counsel for this litigation (Groehn affidavit), and evidence of email communications between a paralegal at the law firm and registrants about whether they intended to or already had purchased credit monitoring or related services because of the Data Breach (Omran affidavits).

[142] Capital One says all of this evidence is inadmissible hearsay.

[143] As expert evidence is not necessary on this issue, I have not considered the Groehn affidavit is unnecessary.

[144] The Omran affidavit was made by a lawyer at class counsel's firm. Mr. Omran deposes that 27 individuals who registered on counsel's class action website stated that they had purchased credit monitoring or similar services because of the Data Breach. Some identified the product and the cost. The text of each individual response is set out in an exhibit to this affidavit; however, names are not included. The Omran affidavit also exhibits 62 individual responses to an email sent by class counsel in July 2021, informing all registrants that the two years of free credit monitoring would be expiring soon, that a certification hearing was upcoming, and that for the hearing it would be helpful to know if the person had or intended to purchase credit monitoring or credit flagging because of the Data Breach.[6] Again, individual names are not included.

[145] Is such evidence admissible in a certification hearing?

[146] Courts have answered this question differently. In some cases, information provided by potential class members on a law firm registration website has been excluded as hearsay (e.g. *Fresco v. Canadian Imperial Bank of Commerce* (2009),

[6] Capital One argued that the letter is biased in that it invites individuals to incur these expenses in order to further the claim, and exaggerates the risk to them. That is not an objectively reasonable interpretation of the letter. It is communicating information of interest to the group and soliciting information from it.

71 C.P.C. (6th) 97 (Ont. S.C.J.)), but in others it has been admitted (e.g. *Chalmers v. AMO Canada Company*, 2009 BCSC 689 aff'd 2010 BCCA 560). Some courts have concluded that such evidence is not hearsay because it is not tendered for the truth of its contents (that is, not to show that an individual did incur such costs), but only to show that they claim they did: *John Doe v. R*., 2015 FC 236 at paras. 11-13.

[147] While each case turns on its particular facts, it appears that compilations of truly anonymous on-line complaints are generally not admissible to establish some basis in fact at certification: see, for example, *Pollack v. Advanced Medical Optics, Inc.*, 2011 ONSC 850; *Thorpe v. Honda Canada Inc.*, 2010 SKQB 39; *Harris*. Beyond that, admissibility will turn on the nature of the particular evidence and the court's characterization of the purpose for which it is tendered. For example, in *Walter v. Western Hockey League*, 2016 ABQB 588, the survey evidence in issue consisted of substantive interviews by two different individuals of potential class members. Names were anonymized. The evidence from one set of interviews was excluded but the evidence from the other was admitted, based on the expertise of the interviewer, the structure of the questions, and the fact that interview transcripts were provided.

[148] In *Tucci* BCSC, a data breach case similar to this, Masuhara J. found that responses by individuals who registered on class counsel's website about the impact of the data breach on them could satisfy this requirement: at para. 232; see also *Obodo* at para. 237.

[149] The registrants in this case are not truly anonymous: class counsel know their names and Capital One could seek a disclosure order. The Omran affidavit includes the full text of each response, which I have read. The information itself is straightforward: the individual says that they purchased credit protection services as a result of the Data Breach and many also name the particular service and the cost.

[150] I find that this evidence is not hearsay because it is not tendered for the truth of its contents, but to show that two or more individuals have claimed that they incurred certain costs in purchasing additional credit protection because of the Data

Breach. That is all that is required at this stage. Whether class members can actually prove their losses is a matter for trial.

[151] The plaintiff has satisfied the requirements of s. 4(1)(b).

Some Basis in Fact – Common Issues

[152] This statutory requirement requires the plaintiff to show some basis in fact that each proposed common issue actually exists and can be answered in common across the class. A common issue exists if its resolution will avoid duplicative fact-finding or legal analysis, it is a substantial component of each class member's claim that must be resolved to resolve the claim, and success for one class member means success for all, although not necessarily to the same extent: *Finkel* at paras. 22-23. This highlights that the focus of the inquiry, including the assessment of the evidence, again is on the form of the proceeding, not on the merits of the claim.

[153] I have found that the Claim discloses causes of action in negligence, contract, statutory privacy torts, and breach of consumer protection statutes.

[154] The wording that the plaintiff has proposed for the negligence common issues includes a reference to *PIPEDA*, which I have not accepted. The proposed common issues in the negligence claim should track the elements of the tort, framed as follows:

a) Did Capital One owe the Class a duty of care to take reasonable steps to establish, maintain and enforce appropriate security safeguards against a cyberattack and/or limit the exposure of the Class's personal information in the case of a successful cyberattack?

b) If so, did Capital One breach the applicable standard of care?

c) If so, did Capital One's breach of the standard of care cause damage to the Class?

[155] Capital One does not take issue with the negligence common issues beyond saying that there is no compensable loss. Assessment of the existence of a duty of care, and breach of the applicable standard of care all arise from the relationship between Capital One and the Class, and that relationship is the same for all class members. As causation is alleged to arise from the Data Breach, it is also common across the class.

[156] Capital One does not take issue with the proposed common issues relating to the breach of contract claim beyond saying that there is no compensable loss. Reworded to exclude the claims I have not certified, they are:

a) Did Capital One enter into a contract with each member of the Class that included terms relating to their personal information?

b) If so, did Capital One breach the contract?

[157] The evidence shows that the contract is the Agreement, and that it is the same standard form document for each Class member. Whether Capital One breached the contract is an issue that must be decided by interpreting the Agreement, also an issue that is common across the class.

[158] The plaintiff proposes common issues with respect to breach of each of seven consumer protection statutes (excluding Québec) as follows:

a) With respect to residents of British Columbia, did the defendants violate the *Business Practices and Consumer Protection Act*, S.B.C. 2004, c. 2, by making false and misleading representations regarding their security measures?

b) With respect to residents of Ontario, did the defendants violate the *Consumer Protection Act*, R.S.O. 1990, c. C.31, by engaging in unfair and/or unconscionable acts or practices?

c) With respect to residents of Manitoba, did the defendants violate the *Business Practices Act*, C.C.S.M. c. B120, by making false and misleading representations regarding their security measures?

d) With respect to residents of Saskatchewan, did the defendants violate the *Consumer Protection and Business Practices Act*, S.S. 2014, c. C-30.2, by making false and misleading representations regarding their security measures?

e) With respect to residents of Alberta, did the defendants violate the *Fair Trading Act*, R.S.A. 2000, c. F2, by making false and misleading representations regarding their security measures?

f) With respect to residents of Newfoundland and Labrador, did the defendants violate the *Consumer Protection and Business Practices Act*, S.N.L. 2009, c. C-31.1, by making false and misleading representations regarding their security measures?

g) With respect to residents of Prince Edward Island, did the defendants violate the *Business Practices Act*, R.S.P.E.I. 1988, c. B-7 by making false and misleading representations regarding their security measures?

[159] As I have found that only one of the pleaded misrepresentations is capable of founding a consumer protection claim, I would replace the clause, “by making false and misleading representations regarding their security measures with “by failing to designate individuals responsible for network security management of personal information, storing personal information on an unsecured network and server, and failing to encrypt personal information.”

[160] Capital One objects to the final proposed common issue under this heading, which is:

> Did the defendants otherwise breach the Applicable Consumer Legislation as defined in the notice of civil claim?

[161] Capital One submits that this invites an open-ended inquiry not grounded in pleaded material facts. The plaintiff's submissions did not address it. I agree, and do not certify it.

[162] The plaintiff proposes common issues with respect to each of the four pleaded privacy statutes as follows:

a) With respect to residents of British Columbia, did the defendants violate the *BC Privacy Act*, s. 1? If so, how?

b) With respect to residents of Manitoba, did the defendants violate the *Manitoba Privacy Act*, ss. 2-3? If so, how?

c) With respect to residents of Newfoundland & Labrador, did the defendants violate the *Newfoundland Privacy Act*, s. 3-4? If so, how?

d) With respect to residents of Saskatchewan, did the defendants violate the *Saskatchewan Privacy Act*, ss. 2, 3 and 6? If so, how?

[163] Again, Capital One's only objection is that these issues do not "actually exist" without evidence of loss.

[164] I agree with the plaintiff that each of the four questions require scrutiny of Capital One's conduct under each of the pleaded legal regimes. That conduct is the same across the class. The legal issue concerning the meaning of "wilfulness" in the BC, Saskatchewan and Newfoundland and Labrador privacy laws, discussed above, does not change this. Capital One did not suggest that the evidence fails to meet the "some basis in fact" standard.

[165] The plaintiff proposed five common issues relating to remedy and damages, which I have modified to reflect the causes of action I have accepted:

a) Are the defendants liable in damages to the class for negligence, breach of contract, statutory privacy torts, and breach of the applicable Consumer Protection legislation?

b) Are the defendants jointly and severally liable for damages to the class pursuant to the applicable Negligence Acts?

c) Can the court assess damages in the aggregate, in whole or in part, for the class? If so, what is the amount of the aggregate damage assessment(s) and who should pay it to the class?

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

e) Should the defendants, or any of them, pay prejudgment and post judgment interest? If so, at what annual interest rate? Should the interest be simple or compound?

[166] Capital One did not take issue with these questions except for c), relating to aggregate damages. It pointed to the fact that aggregate damages are permitted under s. 29 of the *CPA* only if the statutory preconditions set out in s. 29(1)(a) to (c) are met. In particular, s. 29(1)(c) requires that the aggregate award "can reasonably be determined without proof by individual class members".

[167] That means an aggregate monetary award is not available if it depends in any way on evidence of individual class members, including a statistical analysis of the damage suffered by a sample of class members: *Fulawka v. Bank of Nova Scotia,* 2012 ONCA 443 at paras. 135-139. The evidence at this point does not rule out the possibility of an aggregate award, so it should be left for trial.

[168] Mr. Campbell has also pleaded nominal damages for breach of contract. Capital One argues, based on *Babstock*, that a nominal damages claim cannot be a common issue. I do not read *Babstock* as saying this. As Brown J. noted, it was in the unusual circumstances of a claim that expressly disclaimed any remedies based on individual loss that the Court found that the breach of contract claim disclosed no reasonable cause of action:

> [67] The remaining question on breach of contract is whether the plaintiffs' claim should survive as a hollow cause of action that does not support any of the remedies they seek. In my view, it should not. While I agree with my colleague Karakatsanis J. that declaratory relief and nominal damages are available in theory as remedies for breach of contract, a reasonable claim is one that has a reasonable chance of achieving the outcome that the plaintiff seeks. That is not this claim. To be sure, the circumstances here are unusual. Not only did the plaintiffs plead only gain-based relief and punitive damages, both of which I have concluded are unavailable in the circumstances the plaintiffs also expressly disclaimed remedies quantified on the basis of individual loss. At no point did the plaintiffs argue that their claim should survive because nominal damages are available. In my view, the plaintiffs' breach of contract claim should be assessed on the basis of the questions put before the Court -- namely, whether a gain-based remedy or punitive damages are available in the circumstances. And on that basis, it is obvious that the plaintiffs' breach of contract claim does not disclose a reasonable cause of action. To allow this claim to proceed to trial would simply be to delay the inevitable, and would not reflect a "proportionate procedur[e] for adjudication" (*Hryniak*, at para. 27).

[169] Here, there is no such disclaimer. Mr. Campbell has pleaded damages for breach of contract quantified based on individual loss as well as remedies that are not based on individual loss. I accept the proposed aggregate damages question as a common issue.

Some Basis in Fact – Preferability

[170] The preferability analysis asks whether, in the context of the action as a whole, a class action proceeding is a better way of resolving the common issues than another type of proceeding in light of the goals of access to justice, judicial economy and behaviour modification: *AIC Limited v. Fischer*, 2013 SCC 69 at para. 19.

[171] Capital One does not make any submission on preferability other than its general objection that there is no evidence of a class-wide injury.

[172] Here, the only alternative to a class proceeding is individual actions. Resolution of the common issues, which are complex, will clearly advance the goals of a class action procedure. That is so even if individual inquiries are necessary to address damages. In *Tucci* BCCA, a very similar data breach case, the Court of Appeal approved the certification judge’s reasoning on preferability: at para. 96. I am

satisfied that the plaintiff has shown some basis in fact that a class action is the preferable procedure.

Some Basis in Fact – Suitability of Representative Plaintiff

[173] In order to be a suitable representative, a plaintiff must be able to fairly and adequately represent the class's interests, must have a workable litigation plan, and must not have a conflict with the interests of other class members on the common issues.

[174] Capital One does not object to Mr. Campbell's suitability as a representative plaintiff beyond its general position on proof of loss.

[175] I have reviewed Mr. Campbell's affidavit evidence. It does not mention a litigation plan. A litigation plan is attached as an exhibit to Mr. Omran's affidavit, but he does not say anything about Mr. Campbell's involvement in it or even his awareness of it. Neither party addressed the litigation plan at the hearing.

[176] This is an unfortunate example of class counsel standing in the shoes of the litigants. Although a litigation plan is prepared by counsel, the statute requires that the representative plaintiff produce it. That is an aspect of demonstrating that this person is able to vigorously represent the interest of the class: *Tucci* BCSC para 274. The evidence should establish that a proposed representative plaintiff is aware of and understands the litigation plan.

[177] Absent any objection from Capital One, I am satisfied that Mr. Campbell is a suitable representative plaintiff. His evidence shows some basis in fact that he is a member of the Class and he states unequivocally that he is aware of his obligations as a representative plaintiff and is committed to active involvement in the litigation. I conclude that he is a suitable representative plaintiff.

CONCLUSION

[178] In conclusion, I make the following orders:

a) The action is certified as a multi-jurisdictional class proceeding under the *CPA*;

b) The Class is defined as all Canadians, except residents of Québec, who applied for or were issued a Capital One credit card and were notified by Capital One that their information was compromised in the Data Breach;

c) Duncan Campbell is appointed as representative plaintiff for the Class;

d) The nature of the claims asserted on behalf of the Class are negligence, breach of contract, breach of statutory privacy torts, and breach of consumer protection legislation;

e) The relief sought by the Class is:

i. a declaration that the defendants owed a duty of care to the plaintiff and the Class and breached the standard of care owed to them;

ii a declaration that the defendants are jointly and severally liable with the hacker pursuant to the negligence statutes of British Columbia, Saskatchewan, Ontario and Newfoundland and Labrador;

iii. a declaration that the defendants breached their contract with each Class member;

iv. damages in the amount of $800 million;

v. assessment of aggregate damages;

vi. a reference or directions necessary to determine any issues not determined at the trial of the common issues;

vii. pre-and post-judgement interest;

viii. costs of administering a plan of distribution of the recovery in this action; and

ix. further and other relief as the Court deems just.

f) The common issues are:

Negligence

i. Did Capital One owe the Class a duty of care to take reasonable steps to establish, maintain and enforce appropriate security safeguards against a cyberattack and/or limit the exposure of the Class's personal information in the case of a successful cyberattack?

ii. If so, did Capital One breach the applicable standard of care?

iii. If so, did Capital One's breach of the standard of care cause damage to the Class?

Contract

iv. Did Capital One enter into a contract with each member of the Class that included terms relating to their personal information?

v. If so, did Capital One breach the contract?

Statutory Privacy Torts

vi. With respect to residents of British Columbia, did the defendants violate the *BC Privacy Act*, s. 1? If so, how?

vii. With respect to residents of Manitoba, did the defendants violate the *Manitoba Privacy Act*, ss. 2-3? If so, how?

viii. With respect to residents of Newfoundland & Labrador, did the defendants violate the *Newfoundland Privacy Act*, s. 3-4? If so, how?

ix. With respect to residents of Saskatchewan, did the defendants violate the *Saskatchewan Privacy Act*, ss. 2, 3 and 6? If so, how?

Breach of Consumer Protection Acts

x. With respect to residents of British Columbia, did the defendants violate the *Business Practices and Consumer Protection Act*, S.B.C. 2004, c. 2, by failing to designate individuals responsible for network security management of personal information, storing personal information on an unsecured network and server, and failing to encrypt personal information?

xi. With respect to residents of Ontario, did the defendants violate the *Consumer Protection Act*, R.S.O. 1990, c. C.31, by failing to designate individuals responsible for network security management of personal information, storing personal information on an unsecured network and server, and failing to encrypt personal information, which constitute unfair and/or unconscionable acts or practices?

xii. With respect to residents of Manitoba, did the defendants violate the *Business Practices Act*, C.C.S.M. c. B120, by failing to designate individuals responsible for network security management of personal information, storing personal information on an unsecured network and server, and failing to encrypt personal information?

xiii. With respect to residents of Saskatchewan, did the defendants violate the *Consumer Protection and Business Practices Act*,

S.S. 2014, c. C-30.2, by failing to designate individuals responsible for network security management of personal information, storing personal information on an unsecured network and server, and failing to encrypt personal information?

xiv. With respect to residents of Alberta, did the defendants violate the *Fair Trading Act*, R.S.A. 2000, c. F2, by failing to designate individuals responsible for network security management of personal information, storing personal information on an unsecured network and server, and failing to encrypt personal information?

xv. With respect to residents of Newfoundland and Labrador, did the defendants violate the *Consumer Protection and Business Practices Act*, S.N.L. 2009, c. C-31.1, by failing to designate individuals responsible for network security management of personal information, storing personal information on an unsecured network and server, and failing to encrypt personal information?

xvi. With respect to residents of Prince Edward Island, did the defendants violate the *Business Practices Act*, R.S.P.E.I. 1988, c. B-7 by failing to designate individuals responsible for network security management of personal information, storing personal information on an unsecured network and server, and failing to encrypt personal information?

Remedy and Damages

xvii. Are the defendants liable in damages to the class for negligence, breach of contract, statutory privacy torts, and breach of the applicable consumer protection legislation?

xviii. Are the defendants jointly and severally liable for the damages to the class pursuant to the applicable Negligence Acts?

xix. Can the court assess damages in the aggregate, in whole or in part, for the class? If so, what is the amount of the aggregate damage assessment(s) and who should pay it to the class?

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

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

g) The proceedings in any other proceeding arising from the same facts as those in the present proceeding are stayed, with the exception of the Royer action in Québec (No. 500-06-001010-194); and

h) The defendants must provide the plaintiff with the names and last known addresses of Class members.

[179] I decline to grant the orders sought with respect to notice and opt out process at this time as these matters were not addressed by either party. The parties did not address costs of this application. The parties may address these matters by way of written submission or seek to appear before me for a brief hearing on these issues.

"Iyer J."