No. S-257192
Vancouver Registry

IN THE SUPREME COURT OF BRITISH COLUMBIA

Between

CHARLENE MARANDUK

PLAINTIFF

and

WEALTHSIMPLE INC., WEALTHSIMPLE INVESTMENTS INC., WEALTHSIMPLE TECHNOLOGIES INC., and ABC COMPANY NO. 1

DEFENDANTS

Brought under the *Class Proceedings Act*, RSBC 1996, c 50

NOTICE OF CIVIL CLAIM

This action has been started by the plaintiff for the relief set out in Part 2 below.

If you intend to respond to this action, you or your lawyer must

(a) file a response to civil claim in Form 2 in the above-named registry of this court within the time for response to civil claim described below, and
(b) serve a copy of the filed response to civil claim on the plaintiffs.

If you intend to make a counterclaim, you or your lawyer must

(a) file a response to civil claim in Form 2 and a counterclaim in Form 3 in the above-named registry of this court within the time for response to civil claim described below, and
(b) serve a copy of the filed response to civil claim and counterclaim on the plaintiffs and on any new parties named in the counterclaim.

JUDGMENT MAY BE PRONOUNCED AGAINST YOU IF YOU FAIL to file the response to civil claim within the time for response to civil claim described below.

Time for response to civil claim

A response to civil claim must be filed and served on the plaintiff,

(a) if you reside anywhere in Canada, within 21 days after the date on which a copy of the filed notice of civil claim was served on you,
(b) if you reside in the United States of America, within 35 days after the date on which a copy of the filed notice of civil claim was served on you,
(c) if you reside elsewhere, within 49 days after the date on which a copy of the filed notice of civil claim was served on you, or
(d) if the time for response to civil claim has been set by order of the court, within that time.

THE PLAINTIFF'S CLAIM

Part 1: STATEMENT OF FACTS

Overview

1. Financial institutions collect, store, and control vast amounts of digitized, highly sensitive personal data as a condition of providing financial services. Canadians are legally and practically required to share this sensitive information – including government-issued identification, Social Insurance Numbers, banking details, and other personal identifiers – in order to access and participate in the financial system. In doing so, they rely on financial institutions to implement and maintain robust, reasonable safeguards to protect that information from unauthorized third-party access, theft, and misuse.

2. Because they are entrusted with such sensitive data, financial institutions are especially attractive targets for data hackers and cybercriminals. Financial institutions therefore face a heightened and ongoing duty to prioritize rigorous data security safeguards, proactive cybersecurity development and deployment, data minimization practices, and comprehensive human-factor security training. Cybersecurity is not merely a technical obligation; it is a core issue of personal security and operational integrity, the significance of which is underscored by the quasi-constitutional status of privacy rights in Canada.

3. This action arises from a data breach at Wealthsimple that was identified on August 30, 2025 and publicly disclosed on September 5, 2025, involving the unauthorized access, theft, and compromise of highly sensitive personal information of an undisclosed number of Wealthsimple customers (the "**Wealthsimple Data Breach**"). The breach occurred through the compromise of software provided by a third-party vendor engaged by Wealthsimple.

4. As a consequence of the Wealthsimple Data Breach, the Plaintiff and Class Members have suffered psychological, financial, and other harm, including increased risk of identity theft and fraud, costs of protective measures, and loss of privacy, trust, and sense of security.

The Plaintiff and Class Members

5. The Plaintiff, Charlene Maraduk, is a resident of British Columbia. She opened a chequing account with Wealthsimple in or around October 2021, and later opened an RRSP account. Beginning in or around July 2023, the Plaintiff contacted Wealthsimple on multiple occasions in an attempt to close her Wealthsimple accounts. In or around February 2025, the Plaintiff received an email from Wealthsimple notifying her that all of her accounts with Wealthsimple had been closed.

6. On September 5, 2025, the Plaintiff received an email from Wealthsimple advising that some of her personal information was accessed in the Wealthsimple Data Breach. According to Wealthsimple, the accessed information "may include financial information, such as account numbers, IP address, and/or contact information." Wealthsimple provided the Plaintiff with a code to obtain two years of free credit monitoring and dark-web monitoring, as well as identity theft protection and insurance through Equifax. Wealthsimple further advised the Plaintiff to "make sure to use this code before November 30, 2025 to enable the free services provided by Wealthsimple".

7. The Plaintiff brings this claim on her own behalf and on behalf of all Canadians whose information was accessed in the Wealthsimple Data Breach, including a subclass of individuals who claim to have suffered a pecuniary loss due to the misuse of their Compromised Personal Information accessed in the Wealthsimple Data Breach (the "**Data Misuse Subclass**" and the "**Data Misuse Subclass Members**"), (together, the "**Class**" and the "**Class Members**").

The Defendants

8. The Defendant Wealthsimple Inc. is incorporated under the *Canada Business Corporations Act,* RSC 1985, c C-44 (the "***Canada Business Corporations Act***"). It is extra-provincially registered in British Columbia, with an address for service of 3000 – 1055 Dunsmuir Street, Vancouver, BC, V7X 1K8. Wealthsimple Inc. is a registered portfolio manager in each province and territory of Canada and provides managed investment, trading, and other financial services to individual clients in Canada.

9. The Defendant Wealthsimple Investments Inc. is incorporated under the *Canada Business Corporations Act*. It is extra-provincially registered in British Columbia, with an address for service of 3000 – 1055 Dunsmuir Street, Vancouver, BC, V7X 1K8. Wealthsimple Investments Inc. is a registered investment dealer in each province and territory of Canada and provides savings accounts, chequing accounts, registered savings accounts, access to cryptocurrencies, and self-directed investing to individual clients in Canada.

10. The Defendant Wealthsimple Technologies Inc. is incorporated under the *Canada Business Corporations Act*. It is extra-provincially registered in British Columbia, with an address for service of 3000 – 1055 Dunsmuir Street, Vancouver, BC, V7X 1K8. Wealthsimple Technologies provides technological services, including cloud-based data storage and data management to Wealthsimple Inc., Wealthsimple Investments Inc., and affiliates.

11. Wealthsimple Inc., Wealthsimple Investments Inc., and Wealthsimple Technologies Inc. are collectively "**Wealthsimple**". At all material times, they functioned as a joint enterprise, acting in concert in the development, operation, and delivery of Wealthsimple's financial services. Each entity was an agent of the others for the purposes of the conduct alleged in this claim. Wealthsimple carries on business across Canada, including in British Columbia, by making its financial services available to Canadians in Canada.

12. The Defendant ABC Company No. 1 ("**ABC #1**") is a third-party software vendor and service provider that, at all material times, supplied software and/or technological services that were integrated into Wealthsimple's financial services infrastructure. The identity of ABC #1 is unknown to the Plaintiff but known to Wealthsimple.

Wealthsimple Collected the Plaintiff and Class Members' Personal Information

13. The Plaintiff and Class Members are legal persons who were Wealthsimple customers on or before August 30, 2025, and whose personal information was accessed and exfiltrated in the Wealthsimple Data Breach.

14. To provide financial services to Canadians, Wealthsimple is required to collect certain personal information in compliance with Canadian financial and securities laws, including customer identification obligations and anti–money laundering controls for account onboarding and transactions.

15. As part of opening and maintaining Wealthsimple accounts, and in the course of their dealings with Wealthsimple, the Plaintiff and Class Members provided Wealthsimple with – and Wealthsimple collected, processed, and stored – certain personal information, portions of which were accessed and exfiltrated without their authorization in the Wealthsimple Data Breach, including:

(a) full legal names;

(b) dates of birth;

(c) home addresses;

(d) email addresses;

(e) phone numbers;

(f) Social Insurance Numbers (or other government-issued personal identifiers);

(g) bank or financial account numbers associated with Wealthsimple accounts;

(h) copies of government-issued identification provided during account onboarding; and

(i) Internet Protocol (IP) addresses associated with Wealthsimple account access,

(collectively, the "**Compromised Personal Information**").

16. Wealthsimple, through its agents and employees, requested, collected, processed, and stored the Compromised Personal Information for the purpose of contracting and

providing Wealthsimple's financial services. Wealthsimple collected, processed, and stored the Compromised Personal Information electronically.

Timeline of the Wealthsimple Data Breach

17. On or about August 30, 2025, Wealthsimple detected a data security incident resulting from a supply chain attack. The attack originated from a compromised software package developed by ABC #1 that had been integrated into Wealthsimple's infrastructure, which allowed unauthorized access to and exfiltration of the Compromised Personal Information. As of the date of filing this Notice of Civil Claim, Wealthsimple has not disclosed the identity of ABC #1.

18. On or about September 5, 2025, Wealthsimple publicly disclosed the Wealthsimple Data Breach through, *inter alia*, a statement posted on its website and emails sent to affected clients. Wealthsimple's public statement acknowledged that personal data of less than 1% of its clients had been accessed without authorization.

19. However, the emails did not clearly specify the exact Compromised Personal Information accessed in relation to each Class Member. Instead, the language used was vague and inconsistent. For example, some emails stated:

> "Some of your personal information was accessed. This includes your Social Insurance Number and contact information ...",

while others stated:

> "Some of your personal information was accessed. This may include financial information, such as account numbers, IP address, and/or contact information ...",

and still others stated:

> "Some of your personal information was accessed. This may include the government identification you used when you opened your account, DOB, or your contact information ...".

20. This lack of clarity prevented Class Members from understanding the scope and nature of their own exposure resulting from the Wealthsimple Data Breach. There may

have been other versions of these notification emails containing different or additional content.

21. In response to the Wealthsimple Data Breach, Wealthsimple has offered the Plaintiff and Class Members two-year subscriptions to credit monitoring, dark web monitoring, identity theft protection, and identity theft insurance services administered by Equifax. Wealthsimple advised Class Members that they are required to enrol in these services no later than November 30, 2025 in order to receive them at no cost.

Wealthsimple's Representations as to Safeguarding Client Data

22. Wealthsimple represented and continues to represent to the Plaintiff and Class Members – by way of, *inter alia*, its Client Account Agreement, Privacy Policy, Trust Center/Privacy Management Program, public website statements, Help Centre articles, and related contractual and operational documents – that it would safeguard their sensitive and personal information, including the Compromised Personal Information.

23. The Client Account Agreement and other Wealthsimple customer agreements incorporate and expressly require Wealthsimple to handle clients' information in accordance with its Privacy Policy. The Privacy Policy contains express representations regarding Wealthsimple's security, retention, access controls, personnel practices, and service-provider obligations, including, *inter alia*:

> **We implement safeguards**
>
> We maintain reasonable administrative, technical, and physical safeguards in an effort to protect personal information in our custody and control against unauthorized access, use, modification, and disclosure. We train our employees to keep clients' personal information strictly private and confidential. [...]
>
> [...]
>
> **We don't retain information longer than necessary.**
>
> We have personal information retention processes designed to retain personal information of our clients and prospective clients for no longer than necessary for the purposes set out in this Privacy Policy or to otherwise meet legal requirements.

We require similar safeguards from our service providers.

> Our service providers are transferred the information they need to perform their designated functions and committed to maintaining your confidentiality. Our service providers are not permitted to use your information for any unauthorized purpose. Your personal information may be maintained and processed by our Affiliates and other third party service providers outside of Canada, including Quebec, in the US or other jurisdictions. [...]

24. Wealthsimple's Trust Center, Help Centre guidance, and other public statements emphasize Wealthsimple's commitment to protecting client data. For example, on a webpage entitled "Understanding the security and privacy of your account" accessible through Wealthsimple's Help Centre, Wealthsimple assures clients that it uses "the highest standards of security available" and maintains an organizational Privacy Management Program that provides employee privacy training and support.

25. On a webpage entitled "Protecting your assets is our top priority", Wealthsimple represents that its "data collection policies adhere to strict security controls and regulatory requirements," that "[w]e don't keep your data any longer than we need to," and that "With our Privacy Management Program, all our employees are provided with in-depth privacy training and support."

26. Wealthsimple has further reinforced these representations in its public engineering blog, stating that it views "security as an investment, not just an expense", that it is "committed to safeguarding client data and maintaining trust by continually strengthening our security posture", and that "security is not a one-time effort, but a continuous process of improvement". These statements form part of Wealthsimple's continuing public commitment that it would safeguard its clients' sensitive and personal information, including the Compromised Personal Information.

Wealthsimple was Required by the PIPEDA, BC PIPA,* and *AB PIPA to Safeguard and Limit the Retention of the Compromised Personal Information

27. The *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5 (the "***PIPEDA***") governs, *inter alia*, the collection, use, and disclosure of personal information by private-sector organizations in Canada, including information relating to

clients. It also requires the limitation of retention and provides for the secure destruction or anonymization of personal information no longer needed for its original purpose. The *PIPEDA* is intended to regulate how businesses responsibly manage personal information in the course of commercial activities, promote the accountability of private-sector bodies, and safeguard individual privacy by, among other things, prohibiting the unauthorized disclosure of personal information.

28. Section 5(1) of the *PIPEDA* mandates that organizations comply with the obligations set out in Schedule 1. This includes Principles 5 and 7, which state, *inter alia*:

> **4.5 Principle 5 —Limiting Use, Disclosure, and Retention**
>
> Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfilment of those purposes.
>
> [...]
>
> **4.5.2**
>
> Organizations should develop guidelines and implement procedures with respect to the retention of personal information. These guidelines should include minimum and maximum retention periods. Personal information that has been used to make a decision about an individual shall be retained long enough to allow the individual access to the information after the decision has been made. An organization may be subject to legislative requirements with respect to retention periods.
>
> **4.5.3**
>
> Personal information that is no longer required to fulfil the identified purposes should be destroyed, erased, or made anonymous. Organizations shall develop guidelines and implement procedures to govern the destruction of personal information.
>
> [...]
>
> **4.7 Principle 7 — Safeguards**
>
> Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

4.7.1

The security safeguards shall protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification. Organizations shall protect personal information regardless of the format in which it is held.

4.7.2

The nature of the safeguards will vary depending on the sensitivity of the information that has been collected, the amount, distribution, and format of the information, and the method of storage. More sensitive information should be safeguarded by a higher level of protection. The concept of sensitivity is discussed in Clause 4.3.4.

4.7.3

The methods of protection should include

(a) physical measures, for example, locked filing cabinets and restricted access to offices;

(b) organizational measures, for example, security clearances and limiting access on a "need-to-know" basis; and

(c) technological measures, for example, the use of passwords and encryption.

4.7.4

Organizations shall make their employees aware of the importance of maintaining the confidentiality of personal information.

4.7.5

Care shall be used in the disposal or destruction of personal information, to prevent unauthorized parties from gaining access to the information (see Clause 4.5.3).

29. As a private-sector organization engaged in commercial activities and handling personal information, Wealthsimple was statutorily obligated under the *PIPEDA* to, among other things, adequately protect and limit the retention of the Compromised Personal Information.

30. The *Personal Information Protection Act*, SBC 2003, c 63 (the "***BC PIPA***") governs, *inter alia*, the collection, use, and disclosure of personal information by private sector organizations in British Columbia. For example, sections 34 and 35 of the *BC PIPA* state:

> **Protection of personal information**
>
> 34 An organization must protect personal information in its custody or under its control by making reasonable security arrangements to prevent unauthorized access, collection, use, disclosure, copying, modification or disposal or similar risks.
>
> **Retention of personal information**
>
> 35 (1) Despite subsection (2), if an organization uses an individual's personal information to make a decision that directly affects the individual, the organization must retain that information for at least one year after using it so that the individual has a reasonable opportunity to obtain access to it.
>
> (2) An organization must destroy its documents containing personal information, or remove the means by which the personal information can be associated with particular individuals, as soon as it is reasonable to assume that
>
> > (a) the purpose for which that personal information was collected is no longer being served by retention of the personal information, and
> >
> > (b) retention is no longer necessary for legal or business purposes.

31. As a private-sector organization handling personal information while carrying on business in British Columbia, Wealthsimple was subject to the provisions of the *BC PIPA* for its operations within the province.

32. The *Personal Information Protection Act*, SA 2003, c P-6.5 (the "***AB PIPA***") governs, *inter alia*, the collection, use, and disclosure of personal information by private sector organizations in Alberta. For example, the *AB PIPA* states, *inter alia*:

> **Compliance with Act**
>
> 5 (1) An organization is responsible for personal information that is in its custody or under its control.

(2) For the purposes of this Act, where an organization engages the services of a person, whether as an agent, by contract or otherwise, the organization is, with respect to those services, responsible for that person's compliance with this Act.

(3) An organization must designate one or more individuals to be responsible for ensuring that the organization complies with this Act.

(4) An individual designated under subsection (3) may delegate to one or more individuals the duties conferred by that designation.

(5) In meeting its responsibilities under this Act, an organization must act in a reasonable manner.

(6) Nothing in subsection (2) is to be construed so as to relieve any person from that person's responsibilities or obligations under this Act.

Policies and practices

6 (1) An organization must develop and follow policies and practices that are reasonable for the organization to meet its obligations under this Act.

(2) If an organization uses a service provider outside Canada to collect, use, disclose or store personal information for or on behalf of the organization, the policies and practices referred to in subsection (1) must include information regarding

> (a) the countries outside Canada in which the collection, use, disclosure or storage is occurring or may occur, and
>
> (b) the purposes for which the service provider outside Canada has been authorized to collect, use or disclose personal information for or on behalf of the organization.

[...]

Protection of information

34 An organization must protect personal information that is in its custody or under its control by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure, copying, modification, disposal or destruction.

[...]

Retention and destruction of information

35 (1) An organization may retain personal information only for as long as the organization reasonably requires the personal information for legal or business purposes.

(2) Within a reasonable period of time after an organization no longer reasonably requires personal information for legal or business purposes, the organization must

(a) destroy the records containing the personal information, or

(b) render the personal information non-identifying so that it can no longer be used to identify an individual.

[...]

33. As a private-sector organization handling personal information while carrying on business in Alberta, Wealthsimple was subject to the provisions of the *AB PIPA* for its operations within the province.

The Defendants' Misconduct

34. At all material times, Wealthsimple collected, processed, stored, and was responsible for protecting the Compromised Personal Information.

35. At all material times, the Plaintiff and each of the other Class Members entered into one or more contracts with Wealthsimple in respect of the provision and use of Wealthsimple's financial services. Each of these contracts expressly or by implication incorporated Wealthsimple's Privacy Policy. An object of these contracts was to provide the Plaintiff and Class Members with the assurance and psychological benefit that their personal information, including the Compromised Personal Information, would be collected, processed, and stored by Wealthsimple in a secure and confidential manner, and that such information would be reasonably disposed of or anonymized once it was no longer required for the purposes for which it had been collected.

36. At all material times, the Plaintiff and Class Members were vulnerable to Wealthsimple's demands to provide the Compromised Personal Information as a

condition of contracting Wealthsimple's financial services, and to Wealthsimple's care of the Compromised Personal Information.

37. At all material times, Wealthsimple knew or reasonably ought to have known:

(a) of the facts and occurrences of other data breach attacks, including supply chain attacks, in Canada, and specifically such attacks in the financial sector;

(b) that the Compromised Personal Information could, or was likely to, be accessed in a data breach;

(c) of the highly sensitive nature of the Compromised Personal Information; and

(d) that the Plaintiff and Class Members could suffer financial losses and other harms if an unauthorized party were to access and exfiltrate the Compromised Personal Information.

38. The reasonable expectations of the Plaintiff and Class Members when they provided the Compromised Personal Information to Wealthsimple included, *inter alia*:

(a) Wealthsimple would understand and comply with its obligations under the *PIPEDA* and, for Class Members resident in British Columbia and Alberta, the *BC PIPA* and *AB PIPA*, respectively;

(b) Wealthsimple would collect, process, store, and safeguard the Compromised Personal Information using adequate and up-to-date technical, administrative, and physical security measures, including network security, data encryption, and human-factor controls, and would not make it accessible to unauthorized third parties;

(c) Wealthsimple would implement policies and practices to ensure the Compromised Personal Information was appropriately segmented or compartmentalized to minimize the volume of data accessible in the event of any data breach;

(d) Wealthsimple would retain the Compromised Personal Information for only as long was required to fulfill the purposes for which it was collected;

(e) Wealthsimple would promptly detect and competently investigate any potential breach or security incident affecting the Compromised Personal Information;

(f) Wealthsimple would, upon discovering, or having reasonable grounds to believe, that the Compromised Personal Information had been accessed or exfiltrated by an unauthorized third party:

    i. provide prompt and fulsome notice to the Plaintiff and Class Members regarding the nature and extent of the breach, including the specific information of each Plaintiff and Class Member that was involved in the breach; and

    ii. take reasonable and timely steps to mitigate the impact of the breach on the Plaintiff and Class Members;

(g) Wealthsimple would conduct reasonable due diligence before engaging any third-party vendor or integrating any third-party system into its infrastructure, including assessing the vendor's technical security competence and cybersecurity policies and practices;

(h) Wealthsimple would impose and enforce contractual obligations to ensure that any third-party vendor maintained security protections at least equivalent to those required of Wealthsimple itself; and

(i) Wealthsimple would monitor, audit, and periodically reassess the security posture, competence, and software integrity of its third-party vendors and their systems to ensure that they remained secure and did not create vulnerabilities through which unauthorized third parties could compromise client data.

39. The Plaintiff and Class Members' reasonable expectations were informed by the full context of, and all the circumstances surrounding, the Wealthsimple Data Breach, including but not limited to:

(a) the potential misuse of the Compromised Personal Information if this information was accessed and/or exfiltrated in a data breach, including but not limited to identity theft, fraud, and/or extortion;

(b) the Plaintiff and Class Members were required to supply the Compromised Personal Information to Wealthsimple in order to contract its financial services;

(c) Wealthsimple has increased its profit and internal efficiencies due to its collection, processing, and storage of the Compromised Personal Information in electronic form;

(d) Wealthsimple has increased its profit and internal efficiencies by contracting with various third parties;

(e) Wealthsimple's representations made in, *inter alia*, the policies and other public statements referred to at paragraphs 22-26 of this Notice of Civil Claim:

i. regarding the importance of safeguarding sensitive and personal information, including the Compromised Personal Information; and

ii. that it would safeguard and limit the retention of their sensitive and personal information, including the Compromised Personal Information; and

(f) individuals are increasingly vulnerable to the theft and misuse of their personal information, including but not limited to identity theft, fraud, and/or extortion.

40. Wealthsimple wilfully violated the Plaintiff and Class Members' reasonable expectations of privacy by, *inter alia*:

(a) failing to understand and/or comply with its obligations under the *PIPEDA* and, for Class Members resident in British Columbia and Alberta, the *BC PIPA* and *AB PIPA*, respectively;

(b) collecting, processing, and/or storing the Compromised Personal Information in an inadequate and unreasonable manner, including by:

i. using inadequate and/or out-of-date technical, administrative, and physical security measures, including network security, data encryption, and human-factor controls;

ii. implementing inadequate policies and practices, if any, to ensure that the Compromised Personal Information was appropriately segmented or compartmentalized to minimize the volume of data accessed in the Wealthsimple Data Breach;

iii. failing to destroy and/or anonymize the Compromised Personal Information once the purpose for which it had been collected was fulfilled; and/or

iv. failing to detect and respond to the Wealthsimple Data Breach in a timely manner;

(c) failing to provide prompt and sufficiently detailed notice to some or all Class Members regarding which of their Compromised Personal Information had been accessed and/or exfiltrated in the Wealthsimple Data Breach;

(d) failing to take reasonable and timely steps to mitigate the impact of the Wealthsimple Data Breach once it knew or ought to have known of the intrusion; and/or

(e) failing to ensure ABC #1 maintained protections for the Compromised Personal Information comparable to Wealthsimple's, including by:

i. failing to conduct reasonable due diligence on ABC #1's technical security competence and cybersecurity policies and practices;

ii. failing to impose and/or enforce contractual obligations requiring ABC #1 to maintain security safeguards equivalent to those required of Wealthsimple; and/or

iii. failing to monitor, audit, and periodically reassess the security posture, competence, and software integrity of ABC #1 and its systems.

41. Wealthsimple was reckless for engaging in this conduct because, *inter alia*:

(a) Wealthsimple was aware, or ought reasonably to have been aware, that its failure to implement adequate security safeguards and vendor oversight would jeopardize the Compromised Personal Information, exposing the Plaintiff and Class Members to foreseeable risks of misuse by malicious actors, including identity theft, fraud, and extortion;

(b) Wealthsimple knew or ought to have known, based on industry guidance, privacy legislation, and its own internal policies and privacy statements, that it was required to adopt reasonable, up-to-date, and risk-based security safeguards to prevent such harms;

(c) Wealthsimple knew or ought to have known of the heightened risk that third-party vendors could present to its information systems and client data if not properly vetted, contractually bound, monitored, and audited on an ongoing basis; and/or

(d) Wealthsimple proceeded with conscious disregard for these known and obvious risks to the Plaintiff and Class Members' privacy and security, prioritizing internal efficiencies, cost savings, and expediency over implementing the safeguards, due diligence, and monitoring necessary to protect the Compromised Personal Information.

42. At all material times, Wealthsimple knew or ought to have known that this conduct would violate the privacy of the Plaintiff and Class Members.

43. As a result of this conduct, which was done without the consent of the Plaintiff and Class Members, the Compromised Personal Information was accessed and exfiltrated by an unauthorized third party.

44. At all material times, ABC #1:

(a) knew or ought to have known that its software would handle highly sensitive personal and financial information, the compromise of which posed a foreseeable and significant risk of harm to the Plaintiff and Class Members;

(b) designed, developed, updated, and secured the software platform used by Wealthsimple to, *inter alia*, collect, process, and/or store the Compromised Personal Information;

(c) implemented and maintained inadequate network security architecture, including outdated firewalls, insufficient intrusion detection and prevention systems, and inadequate system access controls;

(d) followed outdated and insufficient cybersecurity and data encryption practices and policies that fell below industry standards for vendors handling sensitive personal information;

(e) failed to conduct timely or sufficiently rigorous vulnerability assessments, penetration testing, or code audits of its software or systems to identify and remediate security flaws before they could be exploited;

(f) failed to notify Wealthsimple promptly and with sufficient detail of any suspected or actual security incident or vulnerability affecting the Compromised Personal Information; and

(g) failed to take all reasonable and timely steps to mitigate the impact of any such incident once discovered.

45. The release or potential release of the Compromised Personal Information in the Wealthsimple Data Breach has created an indefinite real risk of significant harm that the Plaintiff and Class Members will be subject to identity theft, fraud, and extortion. In order to mitigate this risk, some Class Members have purchased, or in the future will purchase, long-term credit monitoring and insurance.

46. The credit monitoring offered by Wealthsimple did not constitute adequate risk mitigation measures because, *inter alia*, the credit monitoring is temporary.

47. As a result of the Wealthsimple Data Breach, the Plaintiff and Class Members live under a continuing and reasonable fear of identity theft, fraud, and extortion. This persistent risk has caused and continues to cause them significant psychological harm, including distress, anxiety, and loss of trust. In particular:

(a) they are powerless to control how the Compromised Personal Information may be used by unknown third parties;

(b) some of the Compromised Personal Information, once exposed, cannot be changed or replaced (e.g., dates of birth and Social Insurance Numbers), easily or at all, leaving Class Members vulnerable for life;

(c) the vagueness of Wealthsimple's notices regarding the specific information accessed exacerbated Class Members' uncertainty and anxiety about the scope of their exposure;

(d) they face ongoing uncertainty as to whether their identities have been compromised, requiring constant vigilance over financial accounts and personal records; and

(e) the Defendants' failure to prevent, detect, and adequately contain the Wealthsimple Data Breach undermined Class Members' trust and sense of privacy, contributing to distress, humiliation, and ongoing mental anguish.

48. Additionally, the Data Misuse Subclass Members continue to suffer additional psychological harm beyond that of the broader Class. In particular:

(a) they experience heightened fear, distress, and anxiety from the misuse of their Compromised Personal Information, including identity theft, fraud, and extortion; and

(b) they endure humiliation and reputational damage arising from third parties having gained and exploited intimate or financial details without their consent.

Harm to the Plaintiff and Class Members

49. As a result of the Defendants' negligence, the Plaintiff and Class Members have suffered loss and/or damage including but not limited to the costs of purchasing long-term credit monitoring and/or insurance.

50. As a result of Wealthsimple's breaches of the Provincial Privacy Acts (defined *infra*), Class Members resident in British Columbia, Saskatchewan, Newfoundland, Manitoba, and Québec have suffered loss and/or damage, including but not limited to:

(a) psychological harm including but not limited to distress, embarrassment, humiliation, anguish, reduced trust, feelings of lost privacy, stress, anxiety, and depression; and

(b) the costs, or anticipated costs, of purchasing credit monitoring and/or insurance.

51. As a result of Wealthsimple's breach of contract, the Plaintiff and Class Members have suffered loss and/or damage, including but not limited to:

(a) psychological harm including but not limited to distress, embarrassment, humiliation, anguish, reduced trust, feelings of lost privacy, stress, anxiety, and depression; and

(b) the costs, or anticipated costs, of purchasing credit monitoring and/or insurance.

52. Additionally, Data Misuse Subclass Members have suffered further loss and/or damage due to the Defendants' negligence, Wealthsimple's breach of contract, and, for Data Misuse Subclass Members resident in the above provinces, Wealthsimple's breaches of the Provincial Privacy Acts, including but not limited to financial losses resulting from identify theft, reputational damages, and/or fraud.

53. The loss and/or damages suffered by the Plaintiff and Class Members were the reasonably foreseeable consequences of the Defendants' tortious conduct.

Part 2: RELIEF SOUGHT

54. The Plaintiff claims on her own behalf and on behalf of the other Class Members:

(a) an order certifying this action as a class proceeding and appointing her as representative plaintiff under the *Class Proceedings Act,* RSBC 1996, c 50 (the "***Class Proceedings Act***");

(b) general and special damages for negligence;

(c) damages under provincial privacy legislation (collectively, the "**Provincial Privacy Acts**") as follows:

i. for Class Members resident in British Columbia, moral, general, and special damages under subsection 1(1) of the *Privacy Act,* RSBC 1996 c 373 (the "***BC Privacy Act***");

ii. for Class Members resident in Saskatchewan, moral, general, and special damages under section 2 of the *Privacy Act,* RSS 1978, c P-24 (the "***SK Privacy Act***");

iii. for Class Members resident in Newfoundland, moral, general, and special damages under section 2 of the *Privacy Act,* RSNL 1990, c P-22 (the "***NFLD Privacy Act***");

iv. for Class Members resident in Manitoba, moral, general, and special damages under section 2 of the *Privacy Act,* CCSM c P125 (the "***Manitoba Privacy Act***"); and

v. for Class Members resident in Québec, compensatory (material) and/or punitive damages under article 1611 of the *Civil Code of Québec*, CQLR c CCQ-1991 (the "***Québec Civil Code***"), article 49 of the *Charter of human rights and freedoms*, CQLR c C-12 (the "***Québec Charter***"), and/or section 93.1 of the *Act respecting the protection of personal information in the private sector*, CQLR c P-39.1 (the "***QC Privacy Act***");

(d) expectation damages, or in the alternative nominal damages, for breach of contract;

(e) punitive damages;

(f) pre-judgment and post-judgment interest under the *Court Order Interest Act*, RSBC 1996, c 79 (the "***Court Order Interest Act***"); and/or

(g) such further and other relief as this Honourable Court may deem just.

Part 3: LEGAL BASIS

55. The Plaintiff and Class Members plead and rely on the *Class Proceedings Act,* the *Court Order Interest Act*, the *Negligence Act*, RSBC 1996, c 318, the Provincial Privacy Acts, the *PIPEDA*, the *BC PIPA*, the *AB PIPA*, *Court Jurisdiction and Proceedings Transfer Act*, SBC 2003, c 28 ("***Court Jurisdiction and Proceedings Transfer Act***"), and the Supreme Court Civil Rules, BC Reg 168/2009 and related enactments.

Negligence - Wealthsimple

56. At all material times, Wealthsimple was in a close and proximate relationship with the Plaintiff and Class Members. The relationship between Wealthsimple and the Plaintiff and Class Members was sufficiently close to ground a duty of care because, *inter alia*:

(a) the Plaintiff and Class Members were vulnerable to Wealthsimple's demands to provide the Compromised Personal Information as a condition of contracting Wealthsimple's financial services;

(b) the Plaintiff and Class Members were vulnerable to Wealthsimple's care of the Compromised Personal Information;

(c) Wealthsimple had a direct, transactional relationship, and a relationship by way of contract, with the Plaintiff and Class Members; and

(d) Wealthsimple collected the Compromised Personal Information from the Plaintiff and Class Members in the course of its business.

57. The duty of care owed by Wealthsimple to the Plaintiff and Class Members is informed by, *inter alia*:

(a) Wealthsimple's obligations under the *PIPEDA* and, for Class Members resident in British Columbia and Alberta, the *BC PIPA* and *AB PIPA*, respectively;

(b) the highly sensitive and personal nature of the Compromised Personal Information; and

(c) the inherent danger and foreseeably significant risk of financial, reputational, and other harms to the Plaintiff and Class Members from the disclosure and/or misuse of the Compromised Personal Information.

58. At all material times, Wealthsimple, as custodian of the Compromised Personal Information and contracted service provider of the Plaintiff and Class Members, owed them a duty of care to, *inter alia*:

(a) understand and comply with its obligations under the *PIPEDA* and, for Class Members resident in British Columbia and Alberta, the *BC PIPA* and *AB PIPA*, respectively;

(b) collect, process, store, and safeguard the Compromised Personal Information using adequate and up-to-date technical, administrative, and physical security measures, including network security, data encryption, and human-factor controls, and not make it accessible to unauthorized third parties;

(c) implement policies and practices to ensure the Compromised Personal Information was appropriately segmented or compartmentalized to minimize the volume of data accessible in the event of any data breach;

(d) retain the Compromised Personal Information for only as long was required to fulfill the purposes for which it was collected;

(e) promptly detect and competently investigate any potential breach or security incident affecting the Compromised Personal Information;

(f) upon discovering, or having reasonable grounds to believe, that the Compromised Personal Information had been accessed or exfiltrated by an unauthorized third party:

i. provide prompt and fulsome notice to the Plaintiff and Class Members regarding the nature and extent of the breach, including the specific information of each Plaintiff and Class Member that was involved in the breach; and

ii. take reasonable and timely steps to mitigate the impact of the breach on the Plaintiff and Class Members;

(g) conduct reasonable due diligence before engaging any third-party vendor or integrating any third-party system into its infrastructure, including assessing the vendor's technical security competence and cybersecurity policies and practices;

(h) impose and enforce contractual obligations to ensure that any third-party vendor maintained security protections at least equivalent to those required of Wealthsimple itself; and

(i) monitor, audit, and periodically reassess the security posture, competence, and software integrity of its third-party vendors and their systems to ensure that they remained secure and did not create vulnerabilities through which unauthorized third parties could compromise client data.

59. By the conduct outlined at, *inter alia*, paragraphs 17, 19-20, and/or 40 of this Notice of Civil Claim, Wealthsimple breached the duty of care that it owed to the Plaintiff and Class Members and was negligent.

Negligence – ABC #1

60. At all material times, ABC #1 was in a close and proximate relationship with the Plaintiff and Class Members. The relationship between ABC #1 and the Plaintiff and Class Members was sufficiently close to ground a duty of care because, *inter alia*:

(a) ABC #1 knew or ought to have known that its software would be used by Wealthsimple to collect, process, and/or store the Compromised Personal Information;

(b) the Plaintiff and Class Members were vulnerable to the safety and integrity of ABC #1's software, including the adequacy of its security measures to safeguard the Compromised Personal Information collected, processed, and stored within it;

(c) ABC #1 knew or ought to have known that the Plaintiff and Class Members had no ability to protect their own interests with respect to the design, implementation, or security of ABC #1's software; and

(d) ABC #1's software was integrated into Wealthsimple's systems for the purpose of handling highly sensitive personal and financial information of the Plaintiff and Class Members.

61. The duty of care owed by ABC #1 to the Plaintiff and Class Members is informed by, *inter alia*:

(a) the highly sensitive and personal nature of the Compromised Personal Information; and/or

(b) the inherent danger and foreseeably significant risk of financial, reputational, and other harms to the Plaintiff and Class Members from the disclosure and/or misuse of the Compromised Personal Information.

62. At all material times, ABC #1, as the entity responsible for designing, developing, updating, and securing software systems used by Wealthsimple to collect, process, and/or store the Compromised Personal Information, owed the Plaintiff and Class Members a duty of care to, *inter alia*:

(a) design, develop, update, and secure its software using reasonable and industry-standard administrative, technical, and physical safeguards;

(b) implement, maintain, and periodically update security measures, policies, and procedures to:

i. safeguard the Compromised Personal Information against unauthorized access, disclosure, use, or modification; and

ii. promptly detect, contain, and respond to breaches of its software;

(c) conduct internal monitoring, auditing, and security testing to detect vulnerabilities in its software before they could be exploited;

(d) notify Wealthsimple promptly and with sufficient detail of any suspected or actual security incident or vulnerability affecting the Compromised Personal Information; and

(e) take all reasonable and timely steps to mitigate the impact of any such incident once discovered.

63. By the conduct outlined at, *inter alia*, paragraphs 17 and/or 44 of this Notice of Civil Claim, ABC #1 breached the duty of care that it owed to the Plaintiff and Class Members and was negligent.

Negligence – Causation and Damages

64. As a result of the Defendants' negligence, the Plaintiff and Class Members have suffered loss and/or damage including but not limited to those described at paragraphs 4, 49, and 52 of this Notice of Civil Claim.

65. At all material times, the Defendants were each in a close and proximate relationship with the Plaintiff and Class Members. The loss and/or damages suffered by the Plaintiff and Class Members were the reasonably foreseeable consequences of the Defendants' negligence.

Breaches of the Provincial Privacy Acts

66. Wealthsimple has breached each of the Provincial Privacy Acts.

67. Through the conduct described at, *inter alia*, paragraphs 17, 19-20, and/or 40 of this Notice of Civil Claim, Wealthsimple breached the reasonable expectations that the Plaintiff and Class Members resident in British Columbia, Saskatchewan, Newfoundland, Manitoba, and Québec had when they provided the Compromised Personal Information to Wealthsimple, as outlined at paragraph 38 of this Notice of Civil Claim. Wealthsimple violated the privacy of these Class Members without a claim of right.

68. Wealthsimple's conduct constitutes a willful violation of the privacy of the Plaintiff and Class Members resident in British Columbia, Saskatchewan, Newfoundland, Manitoba, and Québec because:

(a) this conduct was reckless for the reasons described at paragraph 41 of this Notice of Civil claim; and/or

(b) Wealthsimple knew or ought to have known that this conduct would violate the privacy of the Plaintiff and these Class Members.

69. For the reasons described at paragraphs 67 and 68 of this Notice of Civil Claim, Wealthsimple has breached section 1 of the *BC Privacy Act*, section 2 of the *SK Privacy Act*, and section 3 of the *NFLD Privacy Act*.

70. For the reasons described at paragraph 67 of this Notice of Civil Claim, Wealthsimple has breached section 2 of the *MB Privacy Act*.

71. Through the conduct described at, *inter alia*, paragraphs 19-20 and/or 40(c) of this Notice of Civil Claim, Wealthsimple breached sections 3.5 to 3.8 of the *QC Privacy Act* because Wealthsimple failed to notify Class Members resident in Québec in a timely manner of their specific Compromised Personal Information that was compromised in a way that adequately addressed the risk of serious injury.

72. Through the conduct described at, *inter alia*, paragraphs 17 and/or 40(a)-(b) and (d)-(e) of this Notice of Civil Claim, Wealthsimple breached section 10 of the *QC Privacy Act* because Wealthsimple, as a person carrying on an enterprise, failed to take the security measures necessary and reasonable to ensure the protection of the Compromised Personal Information of Class Members resident in Québec which Wealthsimple collected, used, communicated, and/or kept.

73. Through the conduct described at, *inter alia*, paragraphs 17 and/or 40(a)-(b) and (d)-(e) of this Notice of Civil Claim, Wealthsimple breached article 5 of the *Québec Charter* by violating the right to privacy of Class Members resident in Québec. In particular, Wealthsimple permitted unauthorized access to, and potential use of, their personal information through inadequate security measures, thereby constituting an unlawful interference with their right to respect for privacy and reputational integrity.

74. Through the conduct described at, *inter alia*, paragraphs 17 and/or 40(a)-(b) and (d)-(e) of this Notice of Civil Claim, Wealthsimple breached articles 3, 35-37, and/or 1457 of the *Québec Civil Code* by committing a fault in failing to adequately protect, store, and safeguard the personal information of Class Members resident in Québec.

75. As a result of Wealthsimple's breaches of the Provincial Privacy Acts, Class Members (including Data Misuse Subclass Members) resident in British Columbia,

Saskatchewan, Newfoundland, Manitoba, and Québec have suffered loss and/or damage, including but not limited to those described at paragraphs 4, 47-48, 50, and 52 of this Notice of Civil Claim, and are entitled to damages. In particular:

(a) Class Members resident in British Columbia are entitled to moral, general, and special damages under subsection 1(1) of the *BC Privacy Act*;

(b) Class Members resident in Saskatchewan are entitled to moral, general, and special damages under section 2 of the *SK Privacy Act*;

(c) Class Members resident in Newfoundland are entitled to moral, general, and special damages under section 2 of the *NFLD Privacy Act*;

(d) Class Members resident in Manitoba are entitled to moral, general, and special damages under section 2 of the *MB Privacy Act*; and

(e) Class Members resident in Québec are entitled to compensatory (material) and/or punitive damages under article 1611 of the *Québec Civil Code*, article 49 of the *Québec Charter*, and/or section 93.1 of the *QC Privacy Act*.

Breach of Contract

76. Wealthsimple has breached its contracts with the Plaintiff and Class Members, each of which incorporated Wealthsimple's Privacy Policy, as follows:

(a) Wealthsimple was contractually obligated to "maintain reasonable administrative, technical, and physical safeguards in an effort to protect personal information in [its] custody and control against unauthorized access, use, modification, and disclosure", but failed to do so by reason of the conduct detailed at paragraphs 17 and 40(b), (d), and (e) of this Notice of Civil Claim;

(b) Wealthsimple was contractually obligated to "retain personal information of [its] clients and prospective clients for no longer than necessary for the purposes set out in this Privacy Policy or to otherwise meet legal requirements", but failed to do so by reason of the conduct detailed at subparagraph 40(b)(iii) of this Notice of Civil Claim; and

(c) Wealthsimple was contractually obligated to "require similar [administrative, technical, and physical] safeguards from [its] service providers", but failed to do so by reason of the conduct detailed at subparagraph 40(e) of this Notice of Civil Claim.

77. As a result of Wealthsimple's breach of contract, the Plaintiff and Class Members have suffered loss and/or damage, including but not limited to those described at paragraphs 4, 47-48, and 51-52 of this Notice of Civil Claim, and are entitled to expectation damages or, in the alternative, nominal damages.

Punitive Damages

78. Wealthsimple's conduct, as outlined in this Notice of Civil Claim, was reprehensible, outrageous, and shocking to the values of Canadian society as a whole, such that it should attract an award of punitive damages. In particular, Wealthsimple:

(a) deployed and relied on software designed, developed, updated, and secured by a third-party vendor as part of its core data security infrastructure, thereby exposing the Plaintiff and Class Members' highly sensitive personal information to foreseeable security risks, without implementing reasonable safeguards, oversight, or auditing to ensure that the software was secure and fit for that purpose;

(b) failed to implement and maintain industry-standard cybersecurity practices, including data minimization, proactive intrusion detection, and comprehensive human-factor security training, despite the known and foreseeable risk of cyberattacks;

(c) failed to take reasonable steps to prevent the unauthorized access and exfiltration of the Compromised Personal Information; and

(d) acted with complete disregard for the heightened vulnerability of the Plaintiff and Class Members, who were compelled to entrust their personal information to Wealthsimple as a condition of accessing essential financial services.

79. Wealthsimple's misconduct represents a marked departure from ordinary standards of decent corporate conduct. It warrants condemnation, deterrence, and punishment by way of a substantial punitive damages award, as compensatory damages alone are inadequate to achieve these objectives.

Joint and Several Liability

80. The Defendants are jointly and severally liable for the damages allocable to any of them for their negligence.

Plaintiff's address for service:

Slater Vecchio LLP
1800 - 777 Dunsmuir Street
Vancouver, BC V7Y 1K4

Fax number for service: 604.682.5197

Email address for service: service@slatervecchio.com

Place of trial: Vancouver, BC

The address of the registry is:

800 Smithe Street
Vancouver, BC
V6Z 2E1

Date: September 23, 2025

Signature of lawyer for plaintiff

Anthony A. Vecchio, K.C.
Justin Giovannetti
Jaime M. Sarophim
L.W. Vivian Cheung

Rule 7-1 (1) of the Supreme Court Civil Rules states:

(1) Unless all parties of record consent or the court otherwise orders, each party of record to an action must, within 35 days after the end of the pleading period,

(a) prepare a list of documents in Form 22 that lists

(i) all documents that are or have been in the party's possession or control and that could, if available, be used by any party at trial to prove or disprove a material fact, and

(ii) all other documents to which the party intends to refer at trial, and

(b) serve the list on all parties of record.

Appendix

Part 1: CONCISE SUMMARY OF NATURE OF CLAIM:

This is a claim for damages arising from a data breach at Wealthsimple that was identified on August 30, 2025 and publicly disclosed on September 5, 2025, involving the unauthorized access, theft, and compromise of highly sensitive personal information of an undisclosed number of Wealthsimple customers.

Part 2: THIS CLAIM ARISES FROM THE FOLLOWING:

A personal injury arising out of:

[ ] a motor vehicle accident
[ ] medical malpractice
[ ] another cause

A dispute concerning:

[ ] contaminated sites
[ ] construction defects
[ ] real property (real estate)
[ ] personal property
[x] the provision of goods or services or other general commercial matters
[ ] investment losses
[ ] the lending of money
[ ] an employment relationship
[ ] a will or other issues concerning the probate of an estate
[x] a matter not listed here

Part 3: THIS CLAIM INVOLVES:

[x] a class action
[ ] maritime law
[ ] aboriginal law
[ ] constitutional law
[ ] conflict of laws
[ ] none of the above
[ ] do not know

Part 4:

Class Proceedings Act, RSBC 1996, c 34
Personal Information Protection Act, SBC 2003, c 63
Personal Information Protection and Electronic Documents Act, SC 2000, c 5
Privacy Act, RSBC 1996 c. 373
Privacy Act, RSS 1978, c P-24
Privacy Act, CCSM c P125
Privacy Act, RSNL 1990, c P-22
Civil Code of Québec, CQLR c CCQ-1991, arts. 3,35,36,37 and 1457
Québec Charter of Rights and Freedoms, CQLR c C-12, art. 5

Act respecting the protection of personal information in the private sector, CQLR c P-39.1
Negligence Act, RSBC 1996, c 318
Court Order Interest Act, RSBC 1996, c 79