**CANADA**

**PROVINCE OF QUEBEC**
**DISTRICT OF MONTREAL**

**(Class Actions)**
**SUPERIOR COURT**

**NO:** 500-06-000013-264

**RYAN** [redacted]

Applicant

v.

**TELUS DIGITAL (CDA) INC.** (d.b.a. **Telus Digital**), legal person having its head office at 510 West Georgia Street, 5th Floor, Vancouver, British Columbia, V6B 0M3

and

**TELUS COMMUNICATIONS INC.**, legal person having its head office at 510 West Georgia Street, 5th Floor, Vancouver, British Columbia, V6B 0M3

and

**TELUS CORPORATION**, legal person having its head office at 510 West Georgia Street, 23rd Floor, Vancouver, British Columbia, V6B 0M3

Defendants

## APPLICATION TO AUTHORIZE THE BRINGING OF A CLASS ACTION
(ARTICLES 571 AND FOLLOWING C.C.P.)

**TO ONE OF THE HONOURABLE JUDGES OF THE SUPERIOR COURT, SITTING IN AND FOR THE DISTRICT OF MONTREAL, THE APPLICANT STATES:**

1. Applicant seeks authorization to institute a class action on behalf of the following class of which he is a member:

| **Groupe :** | **Class**: |
|---|---|

| | |
|---|---|
| Toutes les personnes au Canada dont les renseignements personnels ou financiers détenus par Telus (ou par l'un de ses clients, agents, filiales ou sociétés affiliées) ont été compromis dans le cadre de l'« incident de cybersécurité » divulgué le ou vers le 11 mars 2026, ou qui ont reçu une notification de Telus concernant un tel incident de cybersécurité.<br><br>(ci-après le « **groupe** »)<br><br>ou tout autre groupe qui sera déterminé par le Tribunal; | All persons in Canada whose personal or financial information held by Telus (or by one its customers, agents, subsidiaries, or affiliates) was compromised in the "Cybersecurity Incident" disclosed on or around March 11, 2026, or who have received notification from Telus of such a cybersecurity incident.<br><br>(hereinafter the "**Class**")<br><br>or any other class to be determined by the Court; |

## I. THE PARTIES

2. Applicant is a consumer who is subscribed to Telus' mobile services and to the Telus Health service for which he pays approximately $1,500 per year;

3. Applicant communicates the extracts from the *Registraire des entreprises* for the Defendants (collectively referred to herein as "**Telus**") *en liasse* as **Exhibit AP-1**;

4. The Defendants carry on an enterprise within the meaning of the Civil Code. Given the close ties between the Defendants, and considering that their obligations were contracted for the operation of an enterprise, they are presumed solidarily liable for the acts and omissions of the other;

## II. THE ISSUE:

5. On March 12, 2026, Reuters published an article titled: "*Telus says it is investigating hack of its systems*", a copy of which is communicated as **Exhibit AP-2**, stating:

> Canadian telecommunications and business services firm Telus (T.TO), is investigating a cybersecurity incident involving unauthorized access to some of its systems, a company spokesperson said on Thursday.
>
> The ShinyHunters hacking group told Reuters in a message it stole at least 700 terabytes of data from Telus.
> …
>
> Telus is working with cyber forensics experts to support its investigation and with law enforcement, and is "notifying impacted customers, as appropriate," the spokesperson said.
>
> The statement did not address what kind of data was stolen or how

much.

> Samples of the data shared by the hacking group with Reuters suggest the stolen data includes **information related to at least two dozen companies that included personally identifiable information, call data and recordings, FBI background check information and source code spanning multiple business divisions** within the business services and telecommunications company.

6. An article published the same day on the Financial Post website titled "*Canadian telecom Telus says it's investigating a cyber-breach*" provided additional details, as appears from a copy of said article communicated as **Exhibit AP-3**:

> An amorphous extortion group called ShinyHunters contacted Bloomberg News this week claiming they were planning to release a **large amount of data stolen from Telus in August** in a "supply chain attack."
>
> The group said it sent Telus a ransom note in February that requested a payment in Bitcoin. The amount was redacted from the note seen by Bloomberg.
>
> **Data belonging to Telus' customers — which include technology companies and banks — have been exposed in the incident**, the hackers claimed.

7. Another article published the same day on the "BleepingComputer" website provided even more details, including the duration and cause of the breach, Applicant communicating the article titled "*Telus Digital confirms breach after hacker claims 1 petabyte data theft*" as **Exhibit AP-4**:

> Canadian business process outsourcing giant Telus Digital has confirmed it suffered a security incident after threat actors claimed to have stolen nearly **1 petabyte of data from the company in a multi-month breach**.
> …
>
> The breach was carried out by threat actors known as ShinyHunters, who claims to have stolen a wide range of customer data related to Telus' BPO operations, as well as **call records for Telus' consumer telecommunications division**.
>
> BleepingComputer was told in **January** that Telus had suffered a breach and contacted the company with questions, but did not receive a response to our emails at that time.
>
> Yesterday, Telus confirmed that it suffered a breach, stating that it is currently investigating what was stolen and which customers were

affected.

…

"We have implemented **additional security measures** to further safeguard our systems and environment. As our investigation progresses, we are notifying any impacted customers, as appropriate. **The security of our customers' information continues to be our highest priority**."

8. Telus was therefore aware of the breach since at least January 2026, but neglected to inform Class Members;

9. Worse, Telus did not have adequate security measures in place at the time of the data breach;

10. Telus acted with gross negligence in the handling of its cybersecurity, as appears from the following portion of the BleepingComputer article (Exhibit AP-4) stating:

> After learning that Telus was not negotiating with ShinyHunters, BleepingComputer contacted the threat actors with questions about the breach.
>
> According to ShinyHunters, **they breached Telus using Google Cloud Platform credentials discovered in data stolen during the Salesloft Drift breach**.
>
> In the Salesloft Drift breach, threat actors downloaded Salesforce data for 760 companies, including customer support tickets. These support cases were scanned for credentials, authentication tokens, and other secrets, which Mandiant reports were used to breach additional platforms.
>
> **ShinyHunters says that they discovered Google Cloud Platform credentials for Telus in the Drift data and used them to access numerous company systems**, including a large BigQuery instance.
>
> After downloading this data, the threat actors said **they used the cybersecurity tool trufflehog to search within it for additional credentials that allowed them to pivot into other Telus systems and download further data**.
>
> In all, ShinyHunters claims to have stolen close to **1 petabyte of data belonging to the company and many of its customers, many of whom use Telus Digital as a BPO provider for customer support operations**. BleepingComputer has not been able to independently confirm the total size of the stolen data.

> The **threat actor shared the names of 28 well-known companies allegedly impacted by the breach**. However, BleepingComputer will not disclose the names of these companies, as we have been unable to independently confirm whether they were impacted.
>
> The threat actor says that much of the data for these customers relates to BPO services provided by Telus Digital, including customer support and call center outsourcing, agent performance ratings, AI-powered customer support tools, fraud detection and prevention, and content moderation solutions.
>
> However, **they also claim to have stolen source code, FBI background checks, financial information, Salesforce data, and voice recordings of support calls for various companies**.
>
> The breach also reportedly **impacts Telus' telecommunication services, including its consumer fixed-line business. The stolen data for these services allegedly includes detailed call records, voice recordings, and campaign data**.
>
> Sample of the call data records seen by BleepingComputer **include a call's time, duration, number from, number to, and other metadata**, such as for call quality.
>
> Overall, based on text files describing the attack reviewed by BleepingComputer, the types of stolen data appear to vary widely between companies, with many different business functions exposed.

11. Telus' negligence is that once it was informed or aware that it was impacted by the aforementioned Salesloft Drift breach, it should have immediately rotated all of those credentials, but neglected to do so;

12. There is no doubt that Telus was notified that impacted by the Salesloft Drift breach by August 26, 2025, at the latest, because Salesloft Drift confirmed this publicly on its website, as appears from **Exhibit AP-5**:

> **August 26, 2025 at 12:15 PM:** The following is the most recent update regarding the recent security incident concerning the Drift integration with Salesforce: From August 8 to August 18, 2025, a threat actor used OAuth credentials to exfiltrate data from our customers' Salesforce instances. **All impacted customers have been notified**.
>
> Initial findings have shown that the actor's primary objective was to steal credentials, specifically focusing on sensitive information like **AWS access keys, passwords**, and Snowflake-related access tokens. We have determined that this incident did not impact customers who do not use our Drift-Salesforce integration. Based on

> our ongoing investigation, we do not see evidence of ongoing malicious activity related to this incident.
>
> In collaboration with Salesforce, we took immediate action to proactively revoke all active access and refresh tokens for the Drift application. As a result, **administrators must re-authenticate their Salesforce connection to re-enable the integration**. We have also hired a third party digital forensics and incident response (DFIR) firm to assist in the investigation and to ensure all appropriate remediation steps have been taken.

13. By failing to adequately change or rotate credentials (i.e. passwords, API keys, access tokens, SSH keys, database passwords, certificates, etc.) across its systems following the Salesloft Drift breach, Telus was grossly negligent in its cybersecurity management and, as such, liable for the ensuing damages;

14. The breach affected not only Class Members who contracted directly with Telus, but also individuals and companies who are Telus' clients, some of which are listed as "Our Technology Partners" on Telus' website, an extract of which is communicated as **Exhibit AP-6**;

15. Aggravating the issue is that for several months after the data breach, Telus failed to communicate with Class Members, nor did they offer them any form of protection whatsoever;

16. For several months after the data breach, Telus had still not confirmed which database(s) and information was accessed, stolen or compromised, and themselves not communicated with the public directly (no press release, no public statements on their website(s) or social media page(s), or otherwise);

17. Applicant has serious reasons to believe that the data reach includes some or all of the following personal information:

    - First and last name;
    - Personal mailing address;
    - Business mailing address;
    - Health records (Telus Health);
    - Voice recordings;
    - Phone call recordings;
    - Detailed call records
    - Email address;
    - Phone number;
    - Date of Birth; and
    - Credit information, bank account information and other financial information.

18. Telus had the obligation to protect that information and to ensure by all proper and required means that this information is safeguarded from compromise, theft or loss;

19. When a data breach affecting millions of individuals – such as this one – occurs, Telus had the obligation to immediately and accurately notify those impacted in order to help them prevent further fraud, identity theft, financial losses, losses of time, stress and inconvenience;

20. This lawsuit stems from Telus' failure to follow these obligations;

21. Telus has inexplicably waited – and continue to wait – several months before publicly announcing the data breach themselves;

22. Many Class Members who did not read the online articles communicated herewith are still left in the dark about the data breach;

23. As of this date (March 13, 2026), there is no mention whatsoever about the data breach on Telus' various websites and social media accounts;

24. Despite the fact that the data breach was announced in multiple media outlets, Telus never communicated a notice to Class members. This decreased the likelihood that people would be aware of the data breach and was surely intended to minimize the adverse effects of the data breach on Telus' sales and reputation;

25. Telus were negligent in choosing to wait before actually notifying the Class members, leaving them at greater risk of fraud and identity theft, although Telus have and had the proper contact information and financial means in order to quickly reach the Class members;

26. Moreover, Telus failed to confirm that they would indemnify and hold the Class members harmless of any losses or damages suffered as a result of the data vreach;

27. Telus has not offered any credit monitoring nor any amount of insurance reimbursement policy to Class members;

28. Fraud can occur well after the data breach, especially in instances were such a large number of individuals are affected;

29. Telus failed to mandate (and pay for) TransUnion Canada and/or Equifax Canada to automatically activate credit monitoring services or fraud alerts for Class members, putting these Class members at greater risk of fraud;

30. By choosing not to automatically activate both credit agencies' credit monitoring services and by not posting the proper fraud alerts for all Class members (which could have been done quickly by email, text message or regular mail), Telus chose to save money instead of helping protect the Class members. Indeed, there is a fee payable to TransUnion and Equifax Canada for activating credit monitoring services and/or to post a fraud alert but Telus are not offering this and have not paid to

automatically activate these services;

31. Telus sought to impart a false sense of security to the Class members by deceptively downplaying the data breach which involves the private information of several million Class members in Canada;

32. After becoming aware of the data breach, Telus waited an unreasonable, negligent and irresponsible amount of time before starting to contact the Class Members in order to inform them of data breach;

33. Personal information is a valuable commodity. There is a “cyber black-market” available for criminals to openly post personal information on a number of Internet websites in what is known as the “dark web”. This demand increases the likelihood of Class members falling victim to identity theft;

34. As a result of Telus’ inadequate data security, unauthorized third parties / cyber-criminals now possess the private information of Applicant and the Class members;

35. Immediate notice of the breach is essential to obtain the best protection afforded by identity theft protection services. By letting several weeks pass before starting to notify Class members (with many not even informed yet), Telus failed to provide such immediate notice, thus further exacerbating the damages sustained by Applicant and the Class Members;

36. Telus customers (and their clients’ customers) have been and/or will be exposed to fraud and/or identity theft and these Class members have been harmed as a result. Harm to victims of the data breach includes without limitation fraudulent charges on their accounts, disbursements incurred such as for purchasing extra insurance, placing a fraud alert on their credit file, lost time and expenses related to: (a) finding fraudulent charges; (b) cancelling and reissuing cards or bank accounts; (c) credit monitoring and identity theft prevention; (d) imposition of withdrawal and purchase limits on compromised accounts; and (e) the general nuisance and annoyance of dealing with all these issues resulting from the data breach;

37. In addition to the actual monetary losses related to fraud and identity theft, Applicant and the Class members have already and/or will continue to experience stress, anxiety, fear, inconvenience and/or loss of time due to the loss of their personal information, which has made Applicant and the Class members potential targets for fraud and/or identity theft;

38. The Applicant and the Class members have suffered or will suffer certain additional inconveniences and damages including but not limited to the following:

    a) Delays in the processing of any future requests or applications for credit in the future;

    b) The obligation to closely monitor their accounts for possible fraud for all periods

subsequent to the loss of information, for many months or years;

c) The obligation to be even more attentive than normally necessary concerning the communication of their personal information since they are at threat of social engineering and phishing, due to the higher possibility of fraudulent activity caused by Defendants' loss and negligent handling of the information;

d) The obligation to inform their financial institutions of the loss of the information by the Defendants and to deal with said financial institutions in order to reduce risk of fraud as much as possible. In this regard, certain Class members have and/or will close their accounts and open new accounts in order to protect themselves, which will cause further loss of time, inconvenience and costs;

e) Obtaining and reviewing their credit reports, regularly, in order to look for unauthorized transactions or fraud; and

f) A negative effect on their credit score;

39. Many Class members have also paid or will pay certain fees or costs in order to further protect themselves, such as in order to activate a credit monitoring service or in order to purchase fraud insurance or alerts, title or other insurance, to change their personal information such as requesting new driver's licence numbers or Social Insurance Numbers, for credit protection consulting services, etc. Defendants are solely responsible for these costs or fees paid by the Class members and for the inconvenience caused to Class Members in this regard;

40. Applicant invokes *inter alia* the following sections of provincial and federal legislation which apply under the circumstances and Applicant respectfully submits that the mere fact that the personal information was entrusted to the Defendants and subsequently lost by Defendants as detailed above constitutes an unlawful violation of the Class members' fundamental rights, which makes Defendants liable to pay compensatory, moral and punitive damages:

a) Sections 3, 35, 36, 37 and 1621 of the *Civil Code of Quebec*, S.Q. 1991, c. 64*;*

b) Sections 5 and 49 of the *Charter of Human Rights and Freedoms*, CQRL, c. C-12;

c) Sections 1, 2, 3.1 and following, 10, 13 and 17 of the *Act Respecting the Protection of Personal Information in the Private Sector*, CQRL, c. P-39.1;

d) Sections 2, 3, 5 and 11 of the *Personal Information Protection and Electronic Documents Act*, SC 2000, c. 5, as well as its sections 4.1, 4.3, 4.7 to 4.7.4 of its

Schedule 1;

41. Applicant further alleges that Telus did not have a sufficient system or adequate measures in place to adequately protect the risks of its users' personal and highly sensitive information being either: (a) improperly accessed; (b) stolen; and (c) compromised;

42. According to experts, the theft and disclosure of Class members' personal information to third parties, even if just their phone numbers, will cause serious damages, as it appears from a Reader's Digest Canada article titled "*Alarming Things Hackers Can Do with Just Your Cell Phone Number*", communicated as **Exhibit AP-7**:

> After contacting some security experts for their take, it turns out that finding important details about someone's life with just a phone number is incredibly alarmingly easy…and profitable. "In the wrong hands, your cell number can be used to steal your identity and take over almost every online account you have," Veronica Miller, cybersecurity expert at VPNOverview, tells Reader's Digest.
>
> There are several ways a hacker can use a phone number to turn your life upside down. Here are some ways criminals can target you and how to protect yourself.

43. This Court has previously found that "setting up credit monitoring and security alerts, obtaining credit reports, and cancelling cards or closing accounts and replacing them are not "ordinary annoyances, anxieties and fears that people living in society routinely, if sometimes reluctantly, accept" but may amount to something more" (see *Zuckerman c. Target Corporation*, 2017 QCCS 110, para. 73);

## I. <u>CONDITIONS REQUIRED TO AUTHORIZE THIS CLASS ACTION (S. 575 CCP):</u>

### A) THE FACTS ALLEGED APPEAR TO JUSTIFY THE CONCLUSIONS SOUGHT:

44. Applicant reiterates the above allegations in the present section, as though recited at length;

45. Applicant is a consumer who is subscribed to Telus' mobile services and to the Telus Health service for which he pays approximately $1,500 per year;

46. Telus has the Applicant's personal, medical, and financial information (full name, date of birth, phone number, address, email address, and payment information, usage information);

47. The Applicant's relationship with Telus includes and requires Telus to take adequate measures and precautions to safeguard the personal and confidential information, including his full name, email address, physical address and phone number;

48. Telus' obligations towards the Applicant include the protection and non-disclosure of his personal and confidential information;

49. Telus' security measures in place before the breach were clearly insufficient;

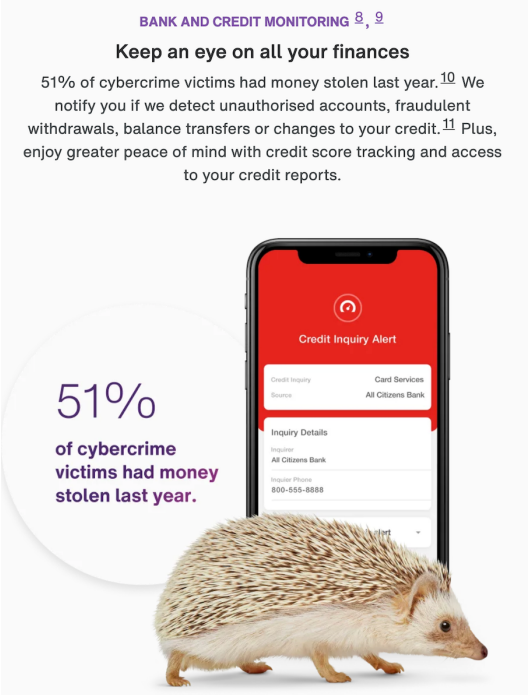
50. Telus management of its IT systems following the Salesloft Drift data breach in August of 2025 was grossly negligent, in that it failed to rotate all of the credentials it knew were or could have been compromised;

51. Applicant fears that his private information is now published on the *darkweb* and available for anyone – including those with bad intentions – to obtain. Quebec's Court of Appeal has noted that such fears could exceed the threshold of normal inconvenience;

52. In fact, Telus itself is well aware that these fears exist and are legitimate, and uses them to boost its sales for data protection services, as appears from Telus' website, an extract of which is communicated as **Exhibit AP-8**:

> ## 86% of Canadians are concerned about their data after a breach[1]
>
> Breaches place your customers' identities into a vulnerable position. When it happens they'll rely on your business to provide the support they need.

53. Telus also offers "dark web monitoring" and "bank and credit monitoring" services that it charges customers for by stating that "***51% of cybercrime victims had money stolen last year***", Telus' webpage communicated as **Exhibit AP-9**:



54. The Applicant's claim for damages is based on breaches by Telus of the following legislation:

    a) Articles 3, 35 and following, and 1458 C.C.Q.;

    b) Articles 5 and 49 of the Quebec *Charter*;

    c) Section 16, 40-42 and 215 and following CPA;

    d) Articles 1, 2, 3.1 and following, 5, 10, 13, 14 and 17 of *An Act respecting the Protection of Personal and Private Information in the Private Sector* (Quebec); and

    e) Sections 5 and following and Schedule 1 of PIPEDA.

55. The Applicant further submits that Telus should be required to pay for credit-monitoring and anti-tracking software due to their breaches and negligence;

56. The Applicant's damages are a direct and proximate result of Telus' omissions, breaches and negligence;

**Punitive Damages:**

57. For all of the reasons more fully detailed above, which are reiterated as though recited at length in the present section, Applicant respectfully submits that Telus was grossly negligent and are liable to pay punitive damages to the Class members;

58. In fact, without limiting the generality of the foregoing, Telus was grossly negligent when they:

    a) did not follow or properly implement an effective data security industry standard to protect the Class members' highly sensitive personal and financial information, which information Telus allowed to be accessed and/or downloaded/stolen by unauthorized third parties;

    b) the management of its systems following the Salesloft Drift data breach in August of 2025, including in failing to rotate all of the credentials it knew were or could have been compromised;

    c) failed to promptly and clearly notify the Applicant and the Class members of the data breach;

    d) failed to properly ensure that Applicant and Class members are protected by credit monitoring services by both Equifax Canada or TransUnion and failing to post fraud alerts on the Class members' credit files immediately after the data breach;

e) failed to timely detect and prevent the data breach itself until several months after it occurred (leaving the Class members' information at risk and “unsecured” for an important amount of time); and

f) failed to offer indemnification for losses suffered by Class members.

59. Therefore, the Applicant is entitled to claim damages, as well as punitive damages in an amount to be determined, pursuant the Quebec *Charter*, the CPA, the Civil Code, and the *Act respecting the protection of personal information in the private sector*, chapter P-39.1, the latter which stipulates:

| | |
|---|---|
| **93.1** Lorsqu’une atteinte illicite à un droit conféré par la présente loi ou par les articles 35 à 40 du *Code civil* cause un préjudice et que cette atteinte est intentionnelle ou résulte **d’une faute lourde**, **le tribunal accorde des dommages-intérêts punitifs d’au moins 1 000 $**. | **93.1.** Where the unlawful infringement of a right conferred by this Act or by articles 35 to 40 of the *Civil Code* causes an injury and the infringement is intentional or **results from a gross fault, the court shall award punitive damages of not less than $1,000.** |

60. Applicant hereby claims **$1000.00** in punitive damages on his behalf and on behalf of each Class member;

61. Considering the above and considering the fact that Telus has violated various laws which have been enacted in order to protect the Class members' personal and/or financial information, Telus us liable to pay punitive damages to all of the Class members due to the loss of private information itself, aside from any other compensatory and moral damages suffered by the Class members;

62. Telus’ above detailed actions qualify the fault as intentional which is a result of wild and foolhardy recklessness in disregard for the rights of the Class members, with full knowledge of the immediate and natural or at least extremely probable consequences that its action would cause to the Class members;

## B) COMMON ISSUES

63. The recourses of the Class members raise identical, similar or related questions of fact or law, namely:

a) Was Telus negligent in the storing and safekeeping of the personal information of the Class members whose information was compromised?

b) Once informed of the breach, did Telus act negligently?

c) Did Telus commit a fault by delaying the notification to Class members that a data breach had occurred?

d) Are Class members entitled to compensatory, moral or punitive damages and in what amounts?

64. All Class members have a common interest in proving the Defendants' liability;

65. In this case, the legal and factual backgrounds at issue are common to all members of the Class;

66. Every member of the Class is entitled to claim damages and to request that Telus pays for credit-monitoring and permanent anti-tracking software. Some Class members may even have the change their phone numbers, which is an enormous inconvenience in today's digital age;

67. Class members are also justified in claiming an aggregate amount for moral damages, punitive damages, and damages troubles and inconvenience;

68. All of the damages to the Class members are a direct and proximate result of the Telus' gross negligence and breaches of privacy laws;

69. Individual questions, if any, pale by comparison to the common questions that are significant to the outcome of the present Application;

**C) THE CLASS**

70. The composition of the Class makes it difficult or impracticable to apply the rules for mandates to take part in judicial proceedings on behalf of others or for consolidation of proceedings;

71. The Applicant conservatively estimates the number of persons included in the class to be in the millions;

72. The names, phone numbers and contact information of all persons included in the Class are not known to the Applicant, however, are all in the possession of the Defendants (but also in possession of the unauthorized third party);

73. Class members are very numerous and are dispersed across the country;

74. These facts demonstrate that it would be impractical, if not impossible, to contact each and every Class member to obtain mandates and to join them in one action;

75. In these circumstances, a class action is the only appropriate procedure for all of the members of the Class to effectively pursue their respective rights and have access to justice without overburdening the court system;

**D) ADEQUATE REPRESENTATIVE**

76. The Applicant requests that he be appointed the status of representative plaintiff for the following main reasons:

a) he is a member of the Class and has a personal interest in seeking the conclusions that he proposes herein;

b) he is competent, in that he has the potential to be the mandatary of the action if it had proceeded under article 91 of the *Code of Civil Procedure*;

c) his interests are not antagonistic to those of other Class members;

77. Additionally, the Applicant respectfully adds that:

a) he has the time, energy, will and determination to assume all the responsibilities incumbent upon him in order to diligently carry out the action;

b) he mandated his attorneys to file the present application for the sole purpose of having his rights, as well as the rights of other Class members, recognized and protected so that they can be compensated and force the Defendants to pay for and offer them credit and fraud monitoring services, as well as an anti-tracking software;

c) he cooperates and will continue to fully cooperate with his attorneys, who have experience in consumer protection and privacy related class actions;

d) he understands the nature of the action.

78. As for identifying other Class members, the Applicant draws certain inferences from the situation and realizes that by all accounts, there is a very significant number of Class members that find themselves in an identical situation, and that it would not be useful to attempt to identify each of them given their sheer numbers;

79. For the above reasons, the Applicant respectfully submits that his interest and competence are such that the present class action could proceed fairly and in the best interest of Class members;

## II. NATURE OF THE ACTION AND CONCLUSIONS SOUGHT

80. The action that the Applicant wishes to institute on behalf of the members of the Class is an action in damages and injunctive relief;

81. The conclusions that the Applicant wishes to introduce by way of an originating application are:

1. **GRANT** the Representative Plaintiff's action against Defendants on behalf of all Class members;

2. **ORDER** the Defendants to permanently provide Class members with credit and fraud monitoring services, as well as anti-tracking software for their devices associated to the compromised information;

3. **CONDEMN** the Defendants to pay the Representative Plaintiff and Class members compensatory damages in an amount to be determined;

4. **CONDEMN** the Defendants to pay the Representative Plaintiff and Class members moral damages and damages for troubles and inconvenience in an amount to be determined;

5. **CONDEMN** the Defendants to pay Class members an amount to be determined on account of punitive damages;

6. **ORDER** the collective recovery of all damages to the Class members;

7. **CONDEMN** the Defendants to pay interest and the additional indemnity on the above sums according to law from the date of service of the *Application to Authorize a Class Action*;

8. **DECLARE** that Defendants are solidarily liable for the monetary condemnation pronounced against the other;

9. **ORDER** the Defendants to deposit in the office of this Court the totality of the sums which forms part of the collective recovery, with interest and costs;

10. **ORDER** that the claims of individual Class members be the object of collective liquidation if the proof permits and alternately, by individual liquidation;

11. **CONDEMN** the Defendants to bear the costs of the present action at all levels, including the cost of all exhibits, notices, the cost of management of claims and the costs of experts, if any, including the costs of experts required to establish the amount of the collective recovery orders;

**FOR THESE REASONS, MAY IT PLEASE THE COURT:**

1. **AUTHORIZE** the bringing of a class action in the form of an originating application in damages, punitive damages and for injunctive relief;

2. **APPOINT** the Applicant the status of Representative Plaintiff of the persons included in the Class herein described as:

| **Groupe :** | **Class**: |
|---|---|
| Toutes les personnes au Canada dont les renseignements personnels ou financiers détenus par Telus (ou par l'un de ses clients, agents, filiales ou sociétés affiliées) ont été compromis dans le cadre de l'« incident de cybersécurité » divulgué le ou vers le 11 mars 2026, ou qui ont reçu | All persons in Canada whose personal or financial information held by Telus (or by one its customers, agents, subsidiaries, or affiliates) was compromised in the "Cybersecurity Incident" disclosed on or around March 11, 2026, or who have received notification from Telus of such a cybersecurity incident. |

| | |
|---|---|
| une notification de Telus concernant un tel incident de cybersécurité. | |
| (ci-après le « **groupe** ») | (hereinafter the "**Class**") |
| ou tout autre groupe qui sera déterminé par le Tribunal; | or any other class to be determined by the Court; |

3. **IDENTIFY** the principal questions of fact and law to be treated collectively as the following:

    a) Was Telus negligent in the storing and safekeeping of the personal information of the Class members whose information was compromised?

    b) Once informed of the breach, did Telus act negligently?

    c) Did Telus commit a fault by delaying the notification to Class members that a data breach had occurred?

    d) Are Class members entitled to compensatory, moral or punitive damages and in what amounts?

4. **IDENTIFY** the conclusions sought by the class action to be instituted as being the following:

    1. **GRANT** the Representative Plaintiff's action against Defendants on behalf of all Class members;

    2. **ORDER** the Defendants to permanently provide Class members with credit and fraud monitoring services, as well as anti-tracking software for their devices associated to the compromised information;

    3. **CONDEMN** the Defendants to pay the Representative Plaintiff and Class members compensatory damages in an amount to be determined;

    4. **CONDEMN** the Defendants to pay the Representative Plaintiff and Class members moral damages and damages for troubles and inconvenience in an amount to be determined;

    5. **CONDEMN** the Defendants to pay Class members an amount to be determined on account of punitive damages;

    6. **ORDER** the collective recovery of all damages to the Class members;

    7. **CONDEMN** the Defendants to pay interest and the additional indemnity on the above sums according to law from the date of service of the

*Application to Authorize a Class Action*;

8. **DECLARE** that Defendants are solidarily liable for the monetary condemnation pronounced against the other;

9. **ORDER** the Defendants to deposit in the office of this Court the totality of the sums which forms part of the collective recovery, with interest and costs;

10. **ORDER** that the claims of individual Class members be the object of collective liquidation if the proof permits and alternately, by individual liquidation;

11. **CONDEMN** the Defendants to bear the costs of the present action at all levels, including the cost of all exhibits, notices, the cost of management of claims and the costs of experts, if any, including the costs of experts required to establish the amount of the collective recovery orders;

5. **ORDER** the publication of a notice to the class members in accordance with article 579 C.C.P. pursuant to a further order of the Court, and **ORDER** the Defendants to pay for said publication costs;

6. **FIX** the delay of exclusion at thirty (30) days from the date of the publication of the notice to the members, date upon which the members of the Class that have not exercised their means of exclusion will be bound by any judgment to be rendered herein;

7. **RENDER** any other order that this Honourable Court shall determine;

8. **THE WHOLE** with costs including publication fees.

Montreal, March 13, 2026

*(s) LPC Avocats*

**LPC AVOCATS**
Me Joey Zukran
276, rue Saint-Jacques, Suite 801
Montreal, Quebec, H2Y 1N3
Tel: 514.379.1572
jzukran@lpclex.com
Counsel for the Applicant

Montreal, March 13, 2026

*(s) Renno Vathilakis Inc.*

**RENNO VATHILAKIS INC.**
Me Michael Vathilakis
145, rue St-Pierre, Suite 201
Montreal, Quebec, H2Y 2L6
Tel: 514 937-1221
mvathilakis@renvath.com
Counsel for the Applicant

**SUMMONS**
(ARTICLES 145 AND FOLLOWING C.C.P)

---

**Filing of a judicial application**

Take notice that the Applicant has filed this Application for Authorization to Institute a Class Action and to Appoint the Status of Representative Plaintiff in the office of the **Superior Court** in the judicial district of **Montreal**.

**Defendant's answer**

You must answer the application in writing, personally or through a lawyer, at the courthouse of Montreal situated at **1 Rue Notre-Dame E, Montréal, Quebec, H2Y 1B6**, within 15 days of service of the Application or, if you have no domicile, residence or establishment in Québec, within 30 days. The answer must be notified to the Applicant's lawyer or, if the Applicant is not represented, to the Applicant.

**Failure to answer**

If you fail to answer within the time limit of 15 or 30 days, as applicable, a default judgment may be rendered against you without further notice and you may, according to the circumstances, be required to pay the legal costs.

**Content of answer**

In your answer, you must state your intention to:

- negotiate a settlement;
- propose mediation to resolve the dispute;
- defend the application and, in the cases required by the Code, cooperate with the Applicant in preparing the case protocol that is to govern the conduct of the proceeding. The protocol must be filed with the court office in the district specified above within 45 days after service of the summons or, in family matters or if you have no domicile, residence or establishment in Québec, within 3 months after service;
- propose a settlement conference.

The answer to the summons must include your contact information and, if you are represented by a lawyer, the lawyer's name and contact information.

**Change of judicial district**

You may ask the court to refer the originating Application to the district of your domicile or residence, or of your elected domicile or the district designated by an agreement with the plaintiff.

If the application pertains to an employment contract, consumer contract or insurance contract, or to the exercise of a hypothecary right on an immovable serving as your main residence, and if you are the employee, consumer, insured person, beneficiary of the insurance contract or hypothecary debtor, you may ask for a referral to the district of your domicile or residence or the district where the immovable is situated or the loss occurred. The request must be filed with the special clerk of the district of territorial jurisdiction after it has been notified to the other parties and to the office of the court already seized of the originating application.

**Transfer of application to Small Claims Division**

If you qualify to act as a plaintiff under the rules governing the recovery of small claims, you may also contact the clerk of the court to request that the application be processed according to those rules. If you make this request, the plaintiff's legal costs will not exceed those prescribed for the recovery of small claims.

**Calling to a case management conference**

Within 20 days after the case protocol mentioned above is filed, the court may call you to a case management conference to ensure the orderly progress of the proceeding. Failing this, the protocol is presumed to be accepted.

**Exhibits supporting the application**

In support of the Application for Authorization to Institute a Class Action and to Appoint the Status of Representative Plaintiff, the Applicant intends to use the following exhibits:

**Exhibit AP-1:** *En liasse*, extracts from the *Registraire des entreprises* for the Defendants;

**Exhibit AP-2:** March 12, 2026, Reuters article titled: "*Telus says it is investigating hack of its systems*";

**Exhibit AP-3:** March 12, 2026, Financial Post article titled "*Canadian telecom Telus says it's investigating a cyber-breach*";

**Exhibit AP-4:** March 12, 2026, BleepingComputer article titled "*Telus Digital confirms breach after hacker claims 1 petabyte data theft*";

**Exhibit AP-5:** Extract of the Salesloft Drift's website (https://trust.salesloft.com/?uid=Drift%2FSalesforce+Security+Update&utm);

**Exhibit AP-6:** "Our Technology Partners'" section of the Telus website (https://www.telusdigital.com/technology-partners);

**Exhibit AP-7:** Copy of Reader's Digest Canada article titled "*Alarming Things Hackers Can Do with Just Your Cell Phone Number*";

**Exhibit AP-8:** Extract of Telus' webpage: https://www.telus.com/en/online-security/b2b-breach-and-partnerships/data-breaches;

**Exhibit AP-9:** Extract of Telus' webpage: https://www.telus.com/en/online-security/detection.

These exhibits are available on request.

**Notice of presentation of an application**

If the application is an application in the course of a proceeding or an application under Book III, V, excepting an application in family matters mentioned in article 409, or VI of the Code, the establishment of a case protocol is not required; however, the application must be accompanied by a notice stating the date and time it is to be presented.

Montreal, March 13, 2026

*(s) LPC Avocats*

**LPC AVOCATS**
Me Joey Zukran
276, rue Saint-Jacques, Suite 801
Montreal, Quebec, H2Y 1N3
Tel: 514.379.1572
jzukran@lpclex.com
Counsel for the Applicant

Montreal, March 13, 2026

*(s) Renno Vathilakis Inc.*

**RENNO VATHILAKIS INC.**
Me Michael Vathilakis
145, rue St-Pierre, Suite 201
Montreal, Quebec, H2Y 2L6
Tel: 514 937-1221
mvathilakis@renvath.com
Counsel for the Applicant

**NOTICE OF PRESENTATION**
(articles 146 and 574 al. 2 C.P.C.)

**TO: TELUS DIGITAL (CDA) INC.**
510 West Georgia Street, 5th Floor,
Vancouver, British Columbia, V6B 0M3

**TELUS COMMUNICATIONS INC.**
510 West Georgia Street, 5th Floor
Vancouver, British Columbia, V6B 0M3

**TELUS CORPORATION**
510 West Georgia Street, 23rd Floor
Vancouver, British Columbia, V6B 0M3

**Defendants**

**TAKE NOTICE** that Applicant's *Application to Authorize the Bringing of a Class Action* will be presented before the Superior Court at **1 Rue Notre-Dame E, Montréal, Quebec, H2Y 1B6**, on the date set by the coordinator of the Class Action chamber.

**GOVERN YOURSELVES ACCORDINGLY.**

Montreal, March 13, 2026

*(s) LPC Avocats*
**LPC AVOCATS**
Me Joey Zukran
276, rue Saint-Jacques, Suite 801
Montreal, Quebec, H2Y 1N3
Tel: 514.379.1572
jzukran@lpclex.com
Counsel for the Applicant

Montreal, March 13, 2026

*(s) Renno Vathilakis Inc.*
**RENNO VATHILAKIS INC.**
Me Michael Vathilakis
145, rue St-Pierre, Suite 201
Montreal, Quebec, H2Y 2L6
Tel: 514 937-1221
mvathilakis@renvath.com
Counsel for the Applicant