CANADA
PROVINCE DE QUÉBEC
District : Québec
Localité : Québec
Nº de dossier judiciaire : 200-32-712170-256

Date : 2026–03–24
Sentence rendue par : Me Alexandre Luiggi

DROUIN JOCELYNE et CHAPUT HENRI-PAUL c. BANQUE ROYALE DU CANADA

Partie demanderesse Partie défenderesse

SENTENCE ARBITRALE

I. INTRODUCTION

1. Résumé du litige

Le litige porte sur

Le présent arbitrage a pour objet la demande de Mme Jocelyne Drouin et M. Henri-Paul Chaput (ci-après « la partie demanderesse ») contre la Banque Royale du Canada (ci-après « la partie défenderesse » ou « RBC ») concernant le remboursement d'un virement frauduleux.
La partie demanderesse réclame la somme de 5 000,00 $, soit le remboursement d'un virement non autorisé de 1 490,00 $, ainsi que des dommages-intérêts pour les troubles et inconvénients subis et les intérêts, suite au refus de l'institution financière de la dédommager.

2. Historique de la procédure

La séance d'arbitrage a été tenue le 2026-03-24

II. LES FAITS

[1] En date du 17 octobre 2024 en fin de soirée, un virement Interac au montant de 1 490,00 $ a été effectué à partir du compte bancaire de la demanderesse au profit d'une entreprise nommée « Paybilt Inc. ».

[2] La demanderesse constate la transaction le lendemain matin (18 octobre 2024) à la réception d'un courriel de confirmation d'Interac, et communique immédiatement avec la RBC pour signaler la fraude. La banque procède alors au blocage et au changement des mots de passe.

[3] La RBC mène une enquête interne et refuse de rembourser la somme, soutenant que la transaction a été validée de façon conforme. Les journaux de transaction de la banque (pièces D-1 et D-2) indiquent que l'opération a été initiée depuis l'adresse IP 23.239.51.164, que le mot de passe a été réinitialisé, et que la transaction a été authentifiée avec succès à l'aide d'un code d'accès à usage unique transmis vocalement (« MFA OTP VOICE ») au numéro de téléphone cellulaire de la demanderesse.

[4] La demanderesse soutient qu'elle n'a jamais répondu à ces appels et dépose en preuve ses relevés de téléphonie cellulaire (Vidéotron) ainsi que des captures d'écran de son appareil démontrant des appels manqués provenant d'un « Appelant inconnu » aux heures concordant avec la fraude (pièces P-4 et P-16).

[5] Préalablement et subséquemment à cet événement, la demanderesse a effectué plusieurs démarches auprès de la RBC et d'Apple (pièce P-1) pour vérifier la sécurité de ses appareils (tablette et téléphone cellulaire) et de son compte, ayant déjà subi une première fraude (qui avait été remboursée) plus tôt à l'automne 2024.

[6] Insatisfaite de la décision de la RBC, la demanderesse a porté plainte auprès de l'Ombudsman des services bancaires et d'investissement (OSBI). L'OSBI a conclu, en avril 2025, qu'il ne recommandait pas de compensation (pièce P-19), soulignant que les identifiants en ligne avaient été utilisés et que le code à usage unique avait été saisi avec succès, conformément aux conventions de la banque.

[7] Une mise en demeure réclamant 5 000,00 $ a été transmise à la RBC le 13 mai 2025 (pièce P-22), demeurée sans suite favorable.

[8] Une audience s'est tenue le 24 mars 2026. Lors de celle-ci, la demanderesse a réitéré sous serment n'avoir jamais répondu aux appels automatisés de la banque. Le représentant de la défenderesse a, pour sa part, formellement reconnu ne posséder aucune preuve d'une faute active de la demanderesse dans l'utilisation de ses appareils ou la garde de ses informations personnelles.

III. LES POSITIONS DES PARTIES

La partie demanderesse demande :

La demanderesse soutient qu'elle n'a jamais autorisé cette transaction ni communiqué ses informations bancaires à quiconque. Elle plaide avoir été diligente dans la sécurisation de ses appareils (mots de passe, NIP, vérifications avec Apple) et affirme que ses relevés téléphoniques prouvent qu'elle n'a jamais répondu à l'appel automatisé dictant le code de sécurité. Elle réclame le remboursement de la somme fraudée (1 490,00 $) ainsi que 3 510,00 $ pour les troubles, le stress, le temps consacré aux démarches et les intérêts.

La partie défenderesse demande :

La défenderesse plaide l'absence de faute de sa part et demande le rejet total de la demande. En s'appuyant sur ses journaux techniques (pièces D-1 et D-2), elle affirme que son système informatique est infaillible et que la transaction a été parfaitement authentifiée. Elle invoque sa Convention de compte de dépôt et sa Convention d'accès électronique (pièces D-3 et D-4) pour plaider que le client est l'unique responsable de la sécurité de ses identifiants et de ses appareils. Subséquemment, la banque fait valoir que les dommages additionnels réclamés sont exagérés, non corroborés et que la demanderesse n'a pas mitigé ses dommages.

IV. LES QUESTIONS EN LITIGE

Les questions en litige sont les suivantes :

La partie défenderesse (RBC) a-t-elle commis une faute dans le traitement et l'autorisation du virement contesté ?

La partie demanderesse a-t-elle commis une faute ou manqué à ses obligations contractuelles de sécurité (garde des identifiants et appareils) ?

En l'absence de faute prouvée de la banque, la convention de compte exonère-t-elle validement la partie défenderesse de la fraude subie par la partie demanderesse ?

Le cas échéant, les dommages réclamés sont-ils justifiés ?

V. LE DROIT APPLICABLE

Législation :

Code civil du Québec (C.c.Q.) : articles 1375, 1437, 1474, 1613 et 2805.

Loi sur la protection du consommateur (L.p.c.) : articles 10 et 261.

Jurisprudence :

Banque de Montréal c. Santhalingam

Dumont c. BMO Financial Group

Agnew c. Daro Electric

Daméus c. Banque Royale du Canada

VI. ANALYSE

[13] De manière préliminaire, le Tribunal rappelle que la relation entre une banque et son client repose sur une confiance légitime qui impose à l'institution financière un devoir de loyauté, de prudence, de diligence et de vérification.

1. Sur le fardeau de la preuve et l'absence de faute de la demanderesse

[14] La défenderesse refuse de rembourser la transaction frauduleuse au motif que son système informatique a enregistré un succès d'authentification (« MFA OTP VOICE », pièce D-2) à l'aide des identifiants valides de la demanderesse. S'appuyant sur l'arrêt Santhalingam, la banque soutient que l'utilisation de ces codes personnels crée une présomption prima facie (à première vue) que la demanderesse a autorisé la transaction ou manqué à ses obligations de sécurité.

[15] Or, en vertu de l'article 2805 C.c.Q., la bonne foi de la demanderesse se présume. Le Tribunal conclut que la demanderesse réussit à renverser la présomption d'autorisation invoquée par la banque en déposant une preuve matérielle et objective convaincante : les relevés téléphoniques de son fournisseur Vidéotron (pièce P-4) et les captures d'écran de son appareil (pièce P-16).

[16] Bien que la pièce P-16 démontre que des appels ont bel et bien sonné sur l'appareil de la demanderesse à 22h11 et 22h18 (concordant avec les registres de la banque), ceux-ci y sont formellement inscrits comme « manqués ». Le fait que ces appels n'apparaissent pas sur la facture détaillée du fournisseur (pièce P-4) corrobore factuellement qu'ils n'ont pas fait l'objet d'une communication répondue et facturable.

[17] Le Tribunal déduit que la mention « succès » au registre de la banque (pièce D-2) indique uniquement que le fraudeur a réussi à saisir le code sur la plateforme en ligne, code qu'il a vraisemblablement intercepté à l'insu de la demanderesse. La technologie permet en effet de telles interceptions (par exemple, par le piratage d'une boîte vocale où le système automatisé de la banque aurait laissé le message, ou par un logiciel malveillant). Une fois cette présomption renversée, il incombe à la défenderesse de prouver une véritable faute ou implication active de la cliente, ce qu'elle échoue à faire, tel que formellement reconnu par son représentant lors de l'audience.

[18] La jurisprudence établit une distinction cruciale quant au comportement du client. Lorsqu'un client participe activement à la fraude, fait preuve de négligence grossière ou ignore des avertissements clairs de sa banque (comme dans l'affaire Dumont), il enfreint ses obligations. En l'espèce, contrairement à ces situations, la demanderesse n'a eu aucune implication active. Son comportement, notamment ses visites préventives chez Apple (pièce P-1), ne dénote aucune insouciance.

[19] Les tribunaux reconnaissent la possibilité technologique que des processus d'authentification puissent être interceptés par des tiers à l'insu des parties (tel qu'illustré dans l'affaire Agnew). La preuve d'appels manqués rompt tout lien de causalité entre une prétendue négligence de la demanderesse et la fraude subie. Le Tribunal conclut que la demanderesse n'a commis aucune faute contributoire.

2. Sur la validité des clauses d'exonération de la banque

[20] La défenderesse invoque ses conventions de compte et d'accès électronique (pièces D-3 et D-4) pour s'exonérer de toute responsabilité, plaidant que le client est le seul responsable de ses identifiants.

[21] Le Tribunal ne peut retenir cet argument. Dès lors que la preuve démontre que la cliente n'a posé aucun geste ayant causé la fraude, la faille provient nécessairement du processus de la banque ou d'une interception externe. Face à un système informatique client non compromis et en l'absence d'implication de ce dernier, la banque demeure soumise à ses obligations strictes. En autorisant le virement alors que son propre système de transmission du code OTP par appel vocal a pu être déjoué à l'insu de sa cliente, la banque a failli à son devoir de prudence.

[22] Les conventions liant les parties (pièces D-3 et D-4) sont des contrats d'adhésion et de consommation. L'article 1437 C.c.Q. prévoit qu'une clause abusive dans un tel contrat est nulle. Comme l'enseigne l'affaire Daméus, une clause rendant le client automatiquement responsable de transactions frauduleuses dans lesquelles il n'a eu aucune implication est abusive. Opposer ces conventions à la demanderesse pour la tenir responsable d'une faille technologique sans lien de causalité avec ses actes équivaut à l'application d'une telle clause abusive.

[23] De plus, en vertu de l'article 10 L.p.c. (lequel est d'ordre public selon l'article 261 L.p.c.), la banque ne peut utiliser un tel contrat pour se décharger des conséquences des défaillances de son propre système de sécurité. La défenderesse doit donc assumer la perte de cette transaction non autorisée.

3. Sur les dommages réclamés

[24] La partie demanderesse réclame le remboursement de la somme de 1 490,00 $ détournée. Pour les motifs évoqués ci-dessus, cette réclamation est accueillie.

[25] La demanderesse réclame également la somme de 3 510,00 $ à titre de dommages-intérêts pour les troubles, les inconvénients et le temps consacré à ce litige. Bien que le Tribunal comprenne les frustrations et le stress vécus par la demanderesse, il importe de rappeler les règles de droit applicables à ce type de réclamation contractuelle.

[26] En vertu de l'article 1613 C.c.Q., le débiteur (la banque) n'est tenu de réparer que les dommages qui étaient prévisibles au moment de la conclusion du contrat. Dans le cadre d'une convention d'accès électronique à vocation purement économique, le préjudice prévisible d'une faille se limite strictement au dommage matériel, soit la perte financière directe. Les dommages moraux, comme les troubles et inconvénients, sont considérés comme des dommages imprévisibles.

[27] Pour écarter cette limitation et obtenir une compensation pour des dommages imprévisibles, la loi exige de prouver que l'inexécution de la banque résulte d'une faute lourde ou intentionnelle (art. 1613 C.c.Q.), ou d'un manquement à son obligation d'agir de bonne foi (art. 1375 C.c.Q.). Il incombe ainsi à la demanderesse de démontrer un comportement abusif, un refus malicieux, un aveuglement volontaire ou une négligence grossière de la part de l'institution financière.

[28] Or, la bonne foi se présume toujours (art. 2805 C.c.Q.). En l'espèce, la preuve démontre que la banque a appliqué strictement les politiques de sa convention, se fiant (bien qu'erronément sur le plan de l'imputabilité finale) à la présomption d'infaillibilité de ses systèmes technologiques (pièce D-2), sans intention de nuire ni insouciance grossière. La décision de l'OSBI (pièce P-19) corrobore d'ailleurs le fait que le refus initial de la banque, bien qu'incorrect en l'absence de faute prouvée de la cliente, s'appuyait sur une interprétation honnête et courante de ses paramètres de sécurité.

[29] En l'absence de preuve d'une faute lourde ou de mauvaise foi de la défenderesse dans le traitement de la réclamation, l'indemnisation se limite au préjudice matériel prévisible de 1 490,00 $. Le surplus de la demande doit être rejeté.

VII. DÉCISION

[POUR CES MOTIFS, LE TRIBUNAL :

ACCUEILLE en partie la demande ;

CONDAMNE la défenderesse, la Banque Royale du Canada, à payer à la partie demanderesse, Mme Jocelyne Drouin et M. Henri-Paul Chaput, la somme totale de 1 593,84 $(soit 1 490,00$ en capital et 103,84 $ pour les intérêts au taux légal et l'indemnité additionnelle prévus à l'article 1619 du Code civil du Québec depuis la mise en demeure du 13 mai 2025) ;

REJETTE le surplus des conclusions de la demande, notamment la réclamation pour dommages pour troubles et inconvénients ;

CONDAMNE la défenderesse aux frais de justice de la présente instance, lesquels s'élèvent à la somme de 118,00 $.

Longueuil, ce 24 Mars 2026
Lieu Date

Me Alexandre Luiggi
Prénom et nom de l'arbitre

accrédité(e) par le Barreau du Québec

Numéro de membre 320449-9

10e8d891-584d-433d-b9cb-6e1d36d9871c

Signature numérique de 10e8d891-584d-433d-b9cb-6e1d36d9871c
Date : 2026.03.24 17:55:35 -04'00'

Signature