LES ENJEUX DES MODES DE PAIEMENT QUANT À LA PRATIQUE NOTARIALE

Marc Lacoursière

Volume 122, Number 2, 2020

URI: <https://id.erudit.org/iderudit/1082363ar>

DOI: <https://doi.org/10.7202/1082363ar>

[See table of contents](#)

Publisher(s)

Éditions Yvon Blais

ISSN

0035-2632 (print)

2369-6184 (digital)

[Explore this journal](#)

Cite this article

Lacoursière, M. (2020). LES ENJEUX DES MODES DE PAIEMENT QUANT À LA PRATIQUE NOTARIALE. *Revue du notariat*, 122(2), 271–320.
<https://doi.org/10.7202/1082363ar>

LES ENJEUX DES MODES DE PAIEMENT QUANT À LA PRATIQUE NOTARIALE

Marc LACOURSIÈRE*

INTRODUCTION	273
1. Paiements	274
1.1 Typologies des paiements	274
1.1.1 Effets de commerce	275
1.1.1.1 Chèque	275
1.1.1.2 Traite bancaire	277
1.1.2 Transfert électronique de fonds	278
1.1.2.1 Virement bancaire	279
1.1.2.1.1 Paiement de détail	280
1.1.2.1.2 Paiement de grande valeur	282
1.1.2.2 Assyst Paiement	284
1.2 Compensation interbancaire	285
1.2.1 Fonctionnement	286
1.2.2 Nouveaux développements	290

* Professeur titulaire à la Faculté de droit, Université Laval, Québec (Canada), et avocat. L'auteur remercie M^e Brigitte Roy, notaire, chargée d'enseignement et directrice associée du programme de maîtrise en droit notarial, Faculté de droit, Université Laval, M^e Gilles Legault, notaire, M^e Jean-Yves Guimond, notaire, ainsi que Steve Thibodeau, de ACCEO Solutions, pour leurs judicieux conseils. L'auteur remercie également Audrey Houle et Marziyeh Asghar Poor pour leur aide précieuse.

1.2.2.1	Chèque	290
1.2.2.2	Transfert électronique de fonds	295
2.	Erreurs et comportements frauduleux	297
2.1	Paiement	298
2.1.1	Chèque et traite bancaire	298
2.1.1.1	Falsification de l'effet	298
2.1.1.1.1	Falsification de la signature	298
2.1.1.1.2	Endossement frauduleux	299
2.1.1.2	Fraudes et délais de compensation	302
2.1.2	Transferts électroniques de fonds	303
2.1.2.1	Fraude interne	304
2.1.2.2	Fraude d'un tiers	305
2.2	Compte en fidéicommiss	314
	CONCLUSION	320

INTRODUCTION

Les modes de paiement se trouvent actuellement à un carrefour de leur évolution. Utilisé depuis plusieurs siècles, le chèque voit sa popularité s'effriter à grande vitesse au détriment de moyens de paiement électroniques. Les dernières statistiques de l'année 2018 compilées par Paiements Canada, l'organisme responsable de gérer le système de paiement national, sont éloquentes : taux d'utilisation de 3,2 % (en baisse constante), pour une valeur de 39 % du total des paiements¹. Le chèque demeure toutefois utilisé dans un contexte commercial où les entreprises apprécient notamment sa simplicité, le crédit temporaire autorisé par le délai de compensation interbancaire, voire par simple habitude. Bien qu'il ait subi une cure de rajeunissement technologique, il faut reconnaître que ses années sont désormais comptées. Néanmoins, le délai de compensation est une arme à double tranchant puisqu'il augmente le délai de transfert des fonds du tireur au bénéficiaire, prêtant ainsi le flanc aux fraudeurs. Les modes de paiement électroniques, qui se déclinent sous plusieurs aspects (transfert électronique de fonds, cartes, paiement numérique, cryptomonnaie), tentent de pallier les inconvénients des chèques tout en offrant un environnement convivial et sécuritaire. Or, bien que le délai de compensation soit sérieusement diminué, il faut reconnaître que les fraudeurs (pirates) rôdent à l'intérieur des organisations comme dans le cyberspace, que ce soit pour le vol de données personnelles, l'usurpation d'identité ou le détournement de sommes d'argent².

En conséquence, le notaire voit sa pratique évoluer, non seulement par les moyens de paiement qu'il utilise, mais également en ce qui concerne son compte en fidéicommiss. Ses obligations se retrouvent ainsi en pleine mutation. Quelques solutions existent pour favoriser l'efficacité des opérations de paiement, comme l'abandon

1. PAIEMENTS CANADA, *Rapport canadien sur les modes de paiement et les tendances des paiements*, 2019, p. 10, en ligne : <https://www.payments.ca/sites/default/files/canadianpaymentmethodsandtrendsreport_fr.pdf?_ga=2.75732885.1439741137.1579532884-175076693.1560001127>. Ce rapport concerne l'année 2018; à titre comparatif, en 2017, la proportion de transactions par chèque était de 5 % et le volume d'utilisation était de 46 %.
2. À ce sujet, voir la fraude interne survenue au Mouvement Desjardins qui est devenue un cas d'école : *infra*, notes 123 à 128 et le texte correspondant.

du chèque au profit des transferts électroniques de fonds. Le projet Assyst Paiement, conçu sur mesure pour la pratique notariale, représente une solution particulièrement intéressante. Toutefois, l'identification des clients, vecteur important de la fraude, pourrait être bonifiée à l'aide des développements technologiques, comme la biométrie, la cryptographie et la technologie du registre distribué, une identité numérique ainsi que, surtout, une meilleure adéquation de l'encadrement juridique.

Nous présentons en premier lieu les modes de paiement, notamment celui qu'utilise le notaire (1). Par la suite, nous analysons le sujet sensible qu'est la fraude bancaire (2).

1. Paiements

Le paiement est au cœur des transactions commerciales et de consommation. Il a certes évolué au fil des ans, influencé par les développements technologiques (1.1). Depuis plus de 200 ans, les modes de paiement (autres que le paiement comptant) sont compensés sur une base journalière. L'efficacité de la compensation et du règlement des paiements est garante de l'efficacité d'un système de paiement (1.2).

1.1 Typologie des paiements

L'écosystème des paiements canadiens offre un éventail de choix de plus en plus variés. Alors que les dernières années étaient caractérisées par le paiement en argent comptant (espèces), le chèque, les cartes de paiement et les transferts électroniques de fonds, ainsi que les développements technologiques des dernières années ont sensiblement amélioré ces modes de paiement. Selon Paiements Canada, responsable de la mise en œuvre du système de paiement canadien³, l'utilisation du chèque est en déclin drastique, et l'argent comptant est peu utilisé, sauf pour les achats de faibles montants⁴. Le paiement mobile séduit la génération des millénaires; la cryptomonnaie, encore à ses balbutiements et très volatile,

3. *Loi canadienne sur les paiements*, L.R.C. (1985), ch. C-21, art. 5-6.

4. PAIEMENTS CANADA, *Rapport canadien sur les modes de paiement et les tendances des paiements*, 2019, p. 10, en ligne : <https://www.payments.ca/sites/default/files/canadianpaymentmethodsandtrendsreport_fr.pdf?_ga=2.75732885.1439741137.1579532884-175076693.1560001127>.

pourrait offrir des jours prometteurs, surtout si l'État décide d'émettre une telle cryptomonnaie⁵.

Nous présentons, en cette première partie, les effets de commerce puisque les notaires utilisent couramment ce mode de paiement (1.1.1). Nous abordons par la suite les transferts électroniques de fonds (1.1.2).

1.1.1 Effets de commerce

Les effets de commerce, dont le nom à lui seul évoque l'archétype d'un instrument de paiement archaïque et d'un autre siècle, se manifestent encore de nos jours par l'utilisation du chèque et de la traite bancaire. Or, l'usage du chèque est maintenant en net déclin. En effet, le taux d'utilisation est de seulement 3,2 %, ce qui représente 39 % du volume total des paiements⁶. Le montant élevé du volume, soit environ 5 800 \$ en moyenne, indique que le chèque est essentiellement utilisé par le gouvernement, par nombre d'entreprises, particulièrement les petites et moyennes entreprises (PME) et par plusieurs notaires. Il convient d'entreprendre la discussion sur les modes de paiement en présentant le chèque (1.1.1.1) et la traite bancaire (1.1.1.2).

1.1.1.1 Chèque

Considéré dans le monde anglo-saxon comme un effet de commerce, le chèque était d'abord destiné à être négocié entre plusieurs détenteurs préalablement à son dépôt à la banque d'encaissement, à l'instar de la lettre de change. Au fil du temps, et en particulier durant la seconde moitié du XX^e siècle, l'usage a mené les bénéficiaires des chèques à les déposer directement auprès de leur banque. Cet usage a permis au chèque de franchir le pas entre un instrument

5. Pour le moment, la Banque du Canada a indiqué qu'elle n'entend pas émettre une monnaie numérique : FINEXTRA, « Bank of Canada Won't Issue Digital Currency – Yet », 27 février 2020, en ligne : <<https://www.finextra.com/newsarticle/35355/bank-of-canada-wont-issue-digital-currency—yet>>.

6. PAIEMENTS CANADA, *Rapport canadien sur les modes de paiement et les tendances des paiements*, 2019, p. 10, en ligne : <https://www.payments.ca/sites/default/files/canadianpaymentmethodsandtrendsreport_fr.pdf?_ga=2.75732885.1439741137.1579532884-175076693.1560001127>. Ce rapport concerne l'année 2018; à titre comparatif, en 2017, la proportion de transactions par chèque était de 5 % et le volume d'utilisation était de 46 %.

de crédit et un instrument de paiement⁷. Étroitement lié à la relation banque-client, il demeure un moyen convivial pour transférer de la monnaie scripturale. Les divers cas de faux endossements observés au cours des dernières années ont mené les banques vers le chemin de la prudence, cristallisant ainsi la qualité d'instrument de paiement maintenant associé au chèque. Au demeurant, le chèque demeure prisé des PME, qui y trouvent peu de substituts (notamment pour le transfert d'informations accompagnant le paiement), contrairement au consommateur et à la grande entreprise.

Par rapport aux instruments de paiement électroniques, le chèque se singularise à plusieurs égards⁸ : il est tiré sur une banque (ou une caisse populaire)⁹; il est payable à demande, car sa date est la date d'émission, et il est valide pour une durée de six mois¹⁰; il peut être postdaté (ou antidaté), bien que le bénéficiaire ne puisse l'exiger¹¹; il peut être certifié, quoique les banques suggèrent habituellement à leur client l'utilisation d'une traite bancaire (une variante de la lettre de change)¹² et il doit respecter une forme précise, dont une signature manuscrite¹³.

Outre ces caractéristiques, il faut souligner ses avantages et ses inconvénients. Dans le premier cas, notons trois éléments. Premièrement, il est très convivial et simple à utiliser. Deuxième-

-
7. Il est intéressant de noter qu'en France, le chèque est considéré comme un instrument de paiement, et non un effet de commerce, car il est non négociable, sauf à la banque d'encaissement. Ajoutons que si le chèque français est barré, les articles 168-175 de la *Loi sur les lettres de change*, L.R.C. (1985), ch. B-4, permettent également le barrement du chèque (pour empêcher sa négociabilité à une personne autre que la banque), mais cet usage n'est pas utilisé au Canada. Si tel était le cas, les cas de fraude seraient certes diminués.
 8. Voir généralement : Nicole L'HEUREUX et Marc LACOURSIÈRE, *Droit bancaire*, 5^e éd., Montréal, Éditions Yvon Blais, 2017, n^{os} 835-851, p. 642-652. Il faut noter que le chèque est une forme particulière de lettre de change. Il possède ainsi ses règles propres pour plusieurs éléments, les règles générales de la loi s'appliquant aux situations non expressément prévues pour les chèques.
 9. *Loi sur les lettres de change*, L.R.C. (1985), ch. B-4, art. 165(1).
 10. *Loi sur les lettres de change*, L.R.C. (1985), ch. B-4, art. 165(1); ASSOCIATION CANADIENNE DES PAIEMENTS (PAIEMENTS CANADA), *Règle A4 - Effets retournés et réacheminés*, 27 janvier 2020, art. 22(a), en ligne : <<https://www.paiements.ca/sites/default/files/a4fre.pdf>>.
 11. *Loi sur les lettres de change*, L.R.C. (1985), ch. B-4, art. 26d).
 12. Globalement, l'effet de l'opération de certification est similaire à la traite bancaire. Par contre, si la banque refuse la certification, le chèque demeure valide; si la banque refuse de fournir une traite, le tireur devra alors tirer un chèque (non certifié). La certification peut être demandée par le tireur ou le bénéficiaire.
 13. *Loi sur les lettres de change*, L.R.C. (1985), ch. B-4, art. 16(1).

ment, il offre la possibilité au tireur d'émettre un contrordre de paiement¹⁴. Selon les principes de droit cambiaire et de Paiements Canada, le délai ultime correspond au moment où le chèque a été compensé (délai de deux ou trois jours); en pratique, le délai varie selon les politiques des institutions financières. Elles peuvent par exemple déterminer que la fin du délai pourrait être fixée à 15 h ou à 18 h le jour où le chèque a été tiré¹⁵. Troisièmement, il permet au tireur de bénéficier d'un crédit de quelques jours durant le délai de compensation interbancaire. Dans le second cas, il faut reconnaître que la simplicité d'utilisation du chèque comporte comme corollaire la facilité d'en falsifier la date, la signature du tireur ou l'endossement¹⁶.

Le chèque étant un instrument de paiement payable à demande, il comporte, pour le détenteur, le droit de le présenter au paiement¹⁷; il peut être négocié à un autre détenteur¹⁸, mais cet usage est de plus en plus rare. Il existe un usage très canadien de requérir la certification ou le visa de la banque¹⁹. Si les tribunaux attribuent parfois à la certification du chèque des effets analogues à l'acceptation d'une lettre de change²⁰, il ne s'agit pas véritablement d'une acceptation, car le refus de la banque de certifier le chèque n'a pas le même effet qu'un refus de la lettre. La banque est tout à fait libre d'accorder ou non la certification. Si la certification est demandée par son client, la banque pourrait être tenue responsable en cas de refus injustifié entraînant un préjudice. Le chèque peut être certifié à la demande du tireur ou du bénéficiaire²¹. En pratique, la banque offre systématiquement à ses clients une traite bancaire plutôt que la certification du chèque.

1.1.1.2 Traite bancaire

Variante de la lettre de change, la traite bancaire est un ordre de paiement adressé par la banque à elle-même ou à une autre

14. *Loi sur les lettres de change*, L.R.C. (1985), ch. B-4, art. 167a).

15. Voir *infra*, section 1.2.1.

16. Voir *infra*, section 2.1.1.1.

17. *Loi sur les lettres de change*, L.R.C. (1985), ch. B-4, art. 166.

18. *Loi sur les lettres de change*, L.R.C. (1985), ch. B-4, art. 59.

19. La certification est originaire du Canada : *Bank of Baroda, Ltd. c. Punjab National Bank, Ltd.*, [1944] A.C.176, 187 (P.C.); *Gaden c. Newfoundland Savings Bank*, [1899] A.C. 281 (P.C.).

20. Nicole L'HEUREUX et Marc LACOURSIÈRE, *Droit bancaire*, 5^e éd., Montréal, Éditions Yvon Blais, 2017, n° 844, p. 647, note 37 et la jurisprudence correspondante.

21. La certification doit être inscrite sur le chèque, à l'instar de la traite bancaire.

banque²². L'effet est donc émis par la banque et est habituellement fait à ordre. La responsabilité de la banque est celle du tireur d'un instrument dont le tireur et le tiré sont la même personne²³. Concrètement, la traite peut être achetée de la banque émettrice pour le montant désiré par une personne, dont le nom apparaîtra sur la traite, ainsi que le montant et le nom du bénéficiaire. À la suite de la vente de la traite par la banque, celle-ci place l'argent versé par l'acheteur dans un compte spécial dans lequel sera puisé l'argent au moment choisi par le bénéficiaire pour réclamer le paiement. Puisque la banque est la seule partie responsable de l'effet, la traite est considérée comme irrévocable lorsqu'elle est émise et l'acheteur ne peut ainsi émettre de contrordre²⁴. Étant acceptée par la banque qui l'a elle-même émise²⁵, la traite bancaire ne comporte aucune échéance, et la banque n'est donc pas libérée par le défaut de présentation dans un délai raisonnable.

Pour ces raisons, la traite apparaît plus sûre que le chèque certifié, et surtout que le chèque régulier. Il est donc manifeste que le notaire qui reçoit ou désire émettre un chèque pour un montant substantiel devrait, à tout le moins, utiliser une traite bancaire pour respecter son obligation de prudence et de diligence²⁶.

1.1.2 Transfert électronique de fonds

Les transferts électroniques de fonds ont la cote au Canada. En effet, seulement 3,2 % des paiements ont lieu par chèque alors que 21 % des paiements ont lieu en espèces²⁷. Si les consommateurs et les entreprises ont adopté les paiements électroniques depuis bon nombre d'années, certaines PME demeurent hésitantes. Selon ces

22. Benjamin GEVA, « The Autonomy of the Banker's Obligation on Bank Drafts and Certified Cheques », (1994) 73 R. du B. can. 21; Benjamin GEVA, « Irrevocability of Bank Drafts, Certified Cheques and Money Orders », (1986) 65 R. du B. can. 107.

23. *Loi sur les lettres de change*, L.R.C. (1985), ch. B-4, art. 25.

24. Benjamin GEVA, « Irrevocability of Bank Drafts, Certified Cheques and Money Orders », (1986) 65 R. du B. can. 107.

25. *Loi sur les lettres de change*, L.R.C. (1985), ch. B-4, art. 34.

26. *Code de déontologie des notaires*, RLRQ, c. N-3, r. 2, art. 23.

27. PAIEMENTS CANADA, *Rapport canadien sur les modes de paiement et les tendances des paiements*, 2019, p. 10, en ligne : <https://www.payments.ca/sites/default/files/canadianpaymentmethodsandtrendsreport_fr.pdf?_ga=2.75732885.1439741137.1579532884-175076693.1560001127>. L'agent comptant est utilisé pour 21 % du volume des transactions, mais seulement pour 1 % de la valeur.

entreprises, les modes de paiements actuellement offerts sont moins conviviaux et plus chers que les chèques. La somme de renseignements obtenu au sujet de la contrepartie et de la transaction est par ailleurs moindre. Enfin, on peut voir dans cette résistance au changement une illustration de la fracture générationnelle. Paiements Canada a entrepris une réforme en profondeur du système de paiement canadien, en ne misant que sur les paiements électroniques et, surtout, en tentant de résoudre les inquiétudes des PME (1.1.2.1). Au demeurant, les notaires peuvent se prévaloir d'un système de paiement électronique, Assyst Paiement, conçu sur mesure pour leurs besoins (1.1.2.2).

1.1.2.1 Virement bancaire

Un transfert électronique de fonds constitue un ordre de paiement donné par un donneur d'ordre (client) à sa banque de payer un bénéficiaire par l'entremise de la banque de ce dernier. Il s'agit en quelque sorte d'un jeu d'écritures, où la banque du donneur d'ordre débite le compte de son client et où la banque du bénéficiaire crédite le compte du bénéficiaire du virement. Ce type de paiement est considéré comme un transfert de crédit, car le donneur d'ordre amorce le paiement en le « poussant » vers le bénéficiaire²⁸. Le virement peut être transmis de diverses manières, que ce soit oralement ou par écrit (lettre, télécopieur, courriel, message texte, etc.). Le terme « virement » est un concept général qui peut à la fois comprendre un transfert de fonds de grande valeur ou un paiement de moindre valeur, comme une carte de paiement.

Il faut distinguer le mandat de paiement de celui de la relation bancaire au sens général. Dans ce dernier cas, il s'agit d'une relation créancier-débiteur. L'ouverture d'un compte de banque implique que le client peut reprendre les fonds déposés à la banque, soit au comptoir, soit par un ordre de paiement, comme un chèque ou un virement électronique. De son côté, la banque doit honorer les ordres de paiement si la provision est suffisante. L'ordre de paiement donné par un donneur d'ordre est considéré comme un mandat²⁹, et la suite des ordres, de la banque du donneur d'ordre vers la

28. Contrairement au chèque qui est considéré comme un transfert de débit, puisque le bénéficiaire « tire » les fonds vers lui.

29. Nicole L'HEUREUX et Marc LACOURSIÈRE, *Droit bancaire*, 5^e éd., Montréal, Éditions Yvon Blais, 2017, n° 901, p. 680-681; *Compagnie d'assurances générales Co-Operators c. Coop fédérée*, 2019 QCCA 1678, par. 71.

banque du bénéficiaire, constitue un sous-mandat. L'article 1564, al. 2 C.c.Q. prévoit que, pour être libératoire, le paiement doit avoir été accepté par le créancier (bénéficiaire). De nos jours, cette question ne pose habituellement pas problème, mais un cas de figure pourrait être soulevé si un notaire (créancier) refuse de recevoir un paiement électronique et demande d'être payé par chèque³⁰.

D'une manière générale, les paiements sont classifiés selon qu'il s'agit de paiements de détail (1.1.2.1.1) ou de grande valeur, supérieurs à 50 000 \$ (1.1.2.1.2). Par la nature même de sa fonction, le notaire est susceptible de transmettre ou de recevoir ces types de paiement, soit par l'entremise d'un client ou d'un autre notaire.

1.1.2.1.1 Paiements de détail

Les paiements électroniques de détail prennent plusieurs formes : les cartes de paiements (débit ou crédit), le virement bancaire, le paiement mobile voire la cryptomonnaie³¹. Concrètement, les cartes de paiement sont plus prisées pour les montants de quelques milliers de dollars.

S'agissant du paiement par la carte de débit, le titulaire de la carte doit nécessairement posséder un compte bancaire. La carte de débit n'est pas encadrée par la loi³², mais par le *Code de pratique canadien des services de cartes de débit*, qui est un code de pratique volontaire³³. Depuis plusieurs années, ce dernier est partiellement

30. *Héli-Forex Inc. c. Nation Cri de Wemindji*, [2000] R.J.Q. 417, REJB 2000-16648 (C.A.).

31. La cryptomonnaie, comme le Bitcoin, représente un moyen de paiement en développement depuis quelques années, bien qu'il soit de nature très volatile. Cependant, plusieurs pays projettent d'émettre leur propre monnaie virtuelle, appelée cryptomonnaie étatique (*central bank digital currency*), comme la Chine, la Suède, l'Union européenne et le Canada. Ces initiatives devraient assurer une plus grande stabilité à la cryptomonnaie et lui permettre de profiter d'une plus grande popularité. Aux fins de ce texte, nous n'élaborerons pas sur cette monnaie, tout en demeurant conscient qu'elle pourrait prendre de plus en plus d'importance au fil des prochaines années.

32. Cette situation pourrait changer si l'OPC envisage d'assujettir la carte de débit à la *Loi sur la protection du consommateur*, RLRQ, c. P-40.1.

33. AGENCE DE LA CONSOMMATION EN MATIÈRE FINANCIÈRE DU CANADA, *Code de pratique canadien des services de cartes de débit*, 1992 (2004), en ligne : <<https://www.canada.ca/content/dam/canada/financial-consumer-agency/migration/fra/industrie/documents/debitcardcode-fra.pdf>>. Au sujet de ce code, voir : Marc LACOURSIÈRE, « Propositions de réforme pour une protection des titulaires de cartes de débit victimes de transferts de fonds non autorisés », (2009) 54 R.D. McGill 91.

incorporé dans le contrat bancaire entre le titulaire et sa banque, notamment en ce qui concerne l'obligation de conserver la confidentialité du numéro d'identification personnel³⁴. Plus récemment, les banques permettent les transferts de fonds depuis leurs sites Internet ou une application mobile. Du point de vue du notaire, cette méthode paraît intéressante pour le client qui désire lui transférer des fonds ou en recevoir³⁵. La limite permise par le contrat bancaire, de quelques milliers de dollars, peut être revue à la hausse, en accord avec la banque, pour une fin précise.

Quant à la carte de crédit, il ne faut pas nécessairement être titulaire d'un compte bancaire pour en obtenir une. Contrairement à la carte de débit, elle est assujettie à la *Loi sur la protection du consommateur*³⁶, en plus de faire l'objet d'un contrat entre le titulaire et l'émetteur (banque). Pour le commerçant, les frais d'utilisation sont plus importants que pour la carte de débit. Elle est couramment utilisée pour des paiements en ligne³⁷.

Tant la carte de débit que la carte de crédit peuvent être conjuguées à un téléphone cellulaire pour être utilisée à l'aide d'une application comme ApplePay ou SamsungPay, si le marchand possède l'infrastructure requise et si le montant ne dépasse pas une certaine limite (relativement faible). En l'espèce, l'opération de paiement est sécurisée au moyen de la biométrie, que ce soit l'empreinte digitale ou la reconnaissance faciale.

34. *Code de pratique canadien des services de cartes de débit*, art. 5.

35. Notons une nouvelle règle de Paiements Canada, en vigueur depuis le 27 janvier 2020. Elle offre une certaine flexibilité par un processus d'autorisation différée qui élimine la nécessité d'être connecté à un réseau Internet au moment du paiement. Elle vise spécifiquement les transporteurs publics, dont le modèle d'affaires exige une autorisation rapide, qui ont inspiré la conception de cette règle. Les commerçants peuvent fournir leur service avant même que la transaction soit autorisée : ASSOCIATION CANADIENNE DES PAIEMENTS (PAIEMENTS CANADA), *Règle E5 – Échange d'effets de paiement de débit point de service à autorisation différée aux fins de la compensation et du règlement*, 27 janvier 2020, en ligne : <<https://www.paiements.ca/sites/default/files/e5fre.pdf>>.

36. RLRQ, c. P-40.1, art. 118-130.

37. En 2016-2017, 77 % des Québécois utilisaient leur carte de crédit pour une transaction en ligne. Voir également : CEFRIO, « Le commerce électronique au Québec », (2016) 7(5) *NETendances* 2016, p. 12, en ligne : <https://cefrio.qc.ca/media/1224/netendances_2016-le-commerce-electronique-au-quebec.pdf>; CEFRIO, « Services bancaires en ligne », (2019) 10(3) *NETendances* 2019, p. 16, en ligne : <https://cefrio.qc.ca/media/2283/netendances-2019_fascicule_services-bancaires_en_ligne.pdf>.

Ces paiements de détail conviennent pour des montants relativement modestes, comme les honoraires liés à la préparation de la plupart des actes juridiques (contrat de mariage, testaments, etc.). Or, en ce qui concerne les transferts de fonds pour les transactions immobilières ou d'autres paiements de grande valeur, des solutions différentes sont requises.

1.1.2.1.2 Paiements de grande valeur

Alors que le chèque et la traite bancaire sont assujettis à la *Loi sur les lettres de change*³⁸, le transfert électronique de fonds est peu réglementé au Canada. Dans l'arrêt *Marcotte c. Fédération des caisses Desjardins du Québec*, la Cour suprême du Canada a confirmé que ce mode de paiement électronique n'est pas encadré par cette loi³⁹. Au Canada, l'encadrement législatif ne vise que certains modes de paiement de détail, comme la carte de crédit (incluant le paiement mobile) ou la carte prépayée⁴⁰. La carte de débit est encadrée par un code de conduite⁴¹. Les règles de compensation interbancaire de Paiements Canada encadrent certains aspects des virements électroniques, de même que des chèques, mais elles ne s'appliquent qu'entre les membres de Paiements Canada, soit entre les banques, excluant les relations entre le donneur d'ordre et sa banque, de même que celles entre le bénéficiaire et sa banque⁴². Enfin, il faut ajouter que la *Loi sur le recyclage des produits de la criminalité et le financement des activités terroristes*⁴³, et son règlement d'applica-

38. L.R.C. (1985), ch. B-4.

39. *Marcotte c. Fédération des caisses Desjardins du Québec*, 2014 CSC 57, [2014] 2 R.C.S. 805.

40. Il arrive parfois que les juges s'inspirent à la fois des règles du droit commun et de l'article 4A du *Uniform Commercial Code* des États-Unis pour déterminer les obligations des parties : NATIONAL CONFERENCE OF COMMISSIONERS ON UNIFORM STATE LAWS et AMERICAN LAW INSTITUTE, *Uniform Commercial Code*, Article 4A, 1992. Cette loi modèle a été codifiée dans le corpus législatif de tous les États aux États-Unis et peu de décisions ont été rapportées par les tribunaux canadiens concernant les cas d'erreur ou de fraude par transferts électroniques de fonds : *Royal Bank of Canada c. Stangl*, [1992] O.J. No. 378 (Div. Gén. Ont.).

41. AGENCE DE LA CONSOMMATION EN MATIÈRE FINANCIÈRE DU CANADA, *Code de pratique canadien des services de cartes de débit*, 1992 (2004), en ligne : <<https://www.canada.ca/content/dam/canada/financial-consumer-agency/migration/fra/industrie/documents/debitcardcode-fra.pdf>>.

42. Sous réserve que le contrat incorpore de telles règles : *B.M.P. Global Distribution Inc. c. Banque de Nouvelle-Écosse*, 2009 CSC 15, [2009] 1 R.C.S. 504, par. 55-58. En pratique, le contrat bancaire n'incorpore jamais ces règles.

43. L.C. 2000, ch. 17.

tion⁴⁴, visent habituellement l'ensemble des paiements, peu importe leurs caractéristiques. L'encadrement des paiements, assumé par les paliers fédéral et provinciaux, s'assimile à un gruyère, au détriment des clients des banques (consommateurs et entreprises), contrairement à ce qui prévaut en Europe⁴⁵.

Il est important de déterminer les responsabilités de chacun des intervenants dans l'opération de paiement. Bien entendu, le notaire peut tenir le rôle du donneur d'ordre ou du bénéficiaire, selon les circonstances. D'une manière générale, les obligations du donneur d'ordre, de la banque du donneur d'ordre, de la banque du bénéficiaire et du bénéficiaire sont les suivantes⁴⁶. Le donneur d'ordre s'engage à transmettre les fonds détenus dans son compte au bénéficiaire désigné et à assumer le risque d'erreur; en cas de fraude de la part d'un employé, ce dernier sera responsable. Toutefois, si le donneur d'ordre est un notaire qui agit au nom d'un client, il est responsable de l'identification de ce dernier⁴⁷. La banque du donneur d'ordre doit vérifier l'authenticité du client, c'est-à-dire vérifier qu'il est bien l'expéditeur de l'ordre⁴⁸. Elle doit également s'assurer que l'ordre ne comporte aucune anomalie. L'ordre doit être exécuté sans erreur et dans un délai raisonnable. Si le donneur d'ordre émet un contrordre de paiement, il doit respecter les normes en vigueur, mais en pratique, ces virements sont souvent irrévocables. Enfin, la banque doit transférer les fonds au véritable bénéficiaire. Il est reconnu que la banque a une obligation de moyens. La banque du bénéficiaire, mandataire de ce dernier, doit vérifier l'identité du bénéficiaire qui doit recevoir le crédit, exécuter l'ordre et créditer ledit bénéficiaire. Elle doit vérifier l'exactitude de l'ordre et aviser sans délai la banque expéditrice (ou autres banques intermédiaires) de l'anomalie. À défaut, elle engage sa responsabilité. Le

44. *Règlement sur le recyclage des produits de la criminalité et le financement des activités terroristes*, DORS/2002-184.

45. *Directive (UE) 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur, modifiant les directives 2002/65/CE, 2009/110/CE et 2013/36/UE et le règlement (UE) n° 1093/2010, et abrogeant la directive 2007/64/CE*, [2015] J.O. L337/35 [Directive révisée sur les paiements].

46. Pour plus de détails, voir : Nicole L'HEUREUX et Marc LACOURSIÈRE, *Droit bancaire*, 5^e éd., Montréal, Éditions Yvon Blais, 2017, n° 911-930, p. 685-694. Il existe également des banques intermédiaires, mais il n'est pas nécessaire d'en traiter dans le cadre de ce texte.

47. Voir *infra*, section 2.1.2.1.

48. L'autorisation devrait être effectuée par écrit. Au sujet de l'autorisation verbale, voir : *El-Zayed c. Bank of Nova Scotia*, [1988] N.S.J. No. 424, 87 N.S.R. (2d) 171 (N.S. S.C. – T.D.).

bénéficiaire accepte le virement, mais il peut le refuser pour diverses raisons, auquel cas il doit aviser sa banque.

Les principes d'encadrement demeurent les mêmes, peu importe les modalités du transfert, c'est-à-dire que le client transfère au notaire un paiement par carte de débit (pour des montants d'importance modeste) ou virement électronique de fonds par la banque (pour les paiements d'importance majeure). Dans ces cas, la jurisprudence et le contrat bancaire pallient le manque d'encadrement réglementaire.

Au demeurant, certains systèmes de paiement sont conçus pour des fins très précises, comme le système Assyst Paiement.

1.1.2.2 Assyst Paiement

Créé il y a quelques années, Assyst Paiement constitue un mode de transfert de fonds conçu pour répondre aux besoins de la pratique notariale. Développé en collaboration par la Chambre des notaires du Québec et TELUS, cet outil procure plusieurs avantages indéniables. Il permet au notaire de recevoir et de transférer des fonds à partir de son compte en fidéicomis dans une institution financière qui participe au projet⁴⁹. Un coupon est remis au client pour payer le notaire dans son compte bancaire en fidéicomis. En utilisant sa signature numérique Entrust, le notaire peut ensuite payer ses fournisseurs, que ce soit une facture, des honoraires, des frais autorisés au compte d'affaires ou un transfert de fonds entre notaires. Il est aussi possible pour le notaire d'annuler (contremander) son paiement. Cet outil de paiement se caractérise par sa rapidité et sa sécurité. Outre les caractéristiques techniques, la sécurité se manifeste par l'irrévocabilité des paiements, éliminant ainsi les risques causés par les délais de compensation. Comme le souligne le témoignage d'un notaire, « [j]uste se conformer aux règles de pratique et aux délais de compensation bancaire, c'était un vrai casse-tête. Il fallait quasiment tenir un agenda juste pour les

49. Les grandes institutions financières sont bien représentées, car les membres sont les suivants : Mouvement Desjardins, Banque Nationale du Canada, RBC Banque Royale, Banque Laurentienne, Banque TD, Banque Scotia, Banque de Montréal, CIBC, HSBC et Tangerine : TELUS, « Assyst Paiement », mars 2019, en ligne : <https://login.assystrealestate.com/rei/TFE/help/AP-TableMontants-v3_RevSL.pdf>.

échanciers. C'était une course folle contre la montre. Avec Assyst Paiement, tout ça est terminé »⁵⁰.

Si cette plateforme semble attrayante, elle souffre de quelques obstacles. D'abord, bien que les frais d'utilisation soient relativement faibles, il semble constituer un frein à son utilisation par certains notaires. Ensuite, plusieurs notaires préfèrent toujours utiliser les chèques, malgré les inconvénients y attachés. Dans la même veine, le coupon émis par le notaire permet d'inscrire plusieurs informations particulièrement pertinentes, mais celles-ci ne sont pas obligatoires (comme l'objet ou le détail de la transaction). Enfin, l'élément qui apparaît le plus important et qui transcende le domaine notarial est lié à la culture d'entreprise. Simplement exprimé, le milieu juridique est par nature traditionnel et il est difficile de modifier les habitudes. À titre d'illustration, l'informatisation du greffe dans les palais de justice se heurte à une résistance de la part des employés et des juges⁵¹. Il en va de même pour les notaires, car ce logiciel de paiement n'est utilisé que par 25 % à 30 % d'entre eux.

À l'exception d'une période de rodage usuelle à ses débuts, le système ne présente aucun problème majeur et se révèle très fiable. Comme cela est le cas avec les transferts électroniques de fonds, les erreurs ou les fraudes proviennent de l'utilisateur, comme une erreur de saisie ou une erreur de vérification de l'identité du client de la part du notaire.

1.2 Compensation interbancaire

La structure dans laquelle tous les services d'accès et de compensation préliminaires des paiements de moindre et de grande valeur convergent vers la compensation et le règlement final se situe au centre du système canadien des paiements⁵². Nous expliquons

50. TELUS, « Le notaire "techno" », 2019, en ligne : <http://www.telusassyst.com/FR/pdf/assystpaiement_notairetechno_juin2014.pdf>.

51. Isabelle MATHIEU, « La lente route vers la justice sans papier », *Le Soleil*, 17 février 2020, Justice et faits divers.

52. Le processus de paiement ne se termine que si les soldes de règlement disponibles sont suffisants. Le problème de l'insuffisance des fonds au compte de règlement d'un adhérent solvable se résout habituellement par des avances garanties accordées par la Banque du Canada. Si l'institution insolvable ne dispose pas des fonds suffisants pour procéder au règlement, les obligations découlant des chèques et des débits préautorisés sont inversées si cela est possible : (à suivre...)

ci-après le fonctionnement général (1.2.1) et les nouveaux développements (1.2.2).

1.2.1 Fonctionnement

Tous les établissements financiers colligent chaque jour les effets de paiement papier (dont les chèques) qui ont été déposés en succursales, ainsi que les informations qui sont inscrites dans leurs ordinateurs⁵³. L'échange de ces titres est effectué quotidiennement entre les banques. Cette opération de compensation et de règlement a lieu en deux temps.

Dans un premier temps, Paiements Canada, qui est responsable de l'établissement d'un réseau de paiement national au Canada⁵⁴, a mis en place en 1984 le Système automatisé de compensation et de règlement (SACR)⁵⁵. Le SACR fournit un mécanisme de compensation et de règlement en vertu duquel les chèques et les autres titres de paiement sont transmis à partir de l'établissement du déposant et présentés au paiement à l'établissement sur lequel ils sont tirés pour être payés. La chambre de compensation agit comme une sorte de répartiteur des titres à être payés entre les banques. L'objectif est alors de déterminer quel est le solde net (crédit moins débit) dû entre chacune des banques. Un chiffrier électronique permet de calculer les positions mutuelles de chacune des banques vis-à-vis ses consœurs. Les centres de données des membres adhérents sont reliés à un ordinateur central pour la compilation, l'envoi, la réception et la compensation continue des titres de paiement entre les banques.

(...suite)

PAIEMENTS CANADA, *Règlement administratif n° 3 – instruments de paiement et système automatisé de compensation et règlement*, DORS/2003-346, art. 53 à 62 [Règlement administratif n° 3].

53. Les membres peuvent présenter à la compensation interbancaire les titres de paiement autorisés en vertu des règles et des règlements.
54. Paiements Canada facilite le règlement entre les établissements financiers des soldes générés par le mouvement de fonds représentés par les titres de paiement.
55. Ce système peut être défini comme un système électronique de comptabilité de compensation et de règlement utilisant un réseau informatique interactif et en ligne, dans le but de faciliter la compensation et le règlement des divers instruments de paiement, en particulier les chèques. Voir : PAIEMENTS CANADA, *Le système de détail*, 2017, en ligne : <<https://www.paiements.ca/à-propos/nos-systèmes-et-règles/le-système-de-détail>>.

Dans un second temps, le solde net des opérations nationales de compensation est transmis en soirée à la Banque du Canada en vue du règlement entre les comptes des membres adhérents détenus à cette banque centrale. Plus précisément, la Banque du Canada joue un rôle essentiel en ce qu'elle fournit les services de règlement final dans les comptes de règlement détenus par les membres adhérents de Paiements Canada et par les membres de Paiements Canada qui participent directement au Système de transfert de paiements de grande valeur (STPGV, ou *Large Value Transfer System, LVTS*)⁵⁶. En d'autres termes, il s'agit d'un ajustement des comptes bancaires.

Le problème fondamental de la compensation interbancaire découle du délai de compensation : plus le délai est long, plus le risque d'un incident de paiement est important⁵⁷. À titre d'illustration, il peut s'agir d'une erreur de la banque, d'un contordre, d'une faillite ou même d'une fraude. Pour cette raison, les paiements de grande valeur sont compensés plus rapidement, en quelques heures ou en temps réel. Bien qu'elle date du XIX^e siècle, la chambre de compensation s'est modernisée au fil des ans. L'affaire *Herstatt*, dont les faits remontent à 1974, fut certes le catalyseur d'une réforme technique et surtout juridique⁵⁸. Au Canada, les opérations des paiements de grande valeur sont comptabilisées en considérant la date de valeur le jour précédent, de sorte que la date du règlement coïncide avec celle de la compensation.

À l'heure actuelle, et en omettant les développements en cours⁵⁹, les délais de compensation demeurent relativement longs, en particulier pour le traitement des chèques⁶⁰. Selon les circons-

56. Essentiellement, il s'agit des grandes institutions financières canadiennes, incluant le Mouvement Desjardins. Voir généralement : PAIEMENTS CANADA, *Système de grande valeur*, 2017, en ligne : <<https://www.paiements.ca/à-propos/nos-systèmes-et-règles/système-de-grande-valeur>>.

57. Les risques sont variés : il peut s'agir du risque de liquidité, du risque de crédit, du risque systémique ou d'un risque opérationnel.

58. *Delbrueck & Co. c. Manufacturers Hanover Trust Co.*, 609 F.2d 1047 (2nd Cir. 1979) (connue comme étant l'« affaire *Herstatt* »). À ce sujet, voir : Gabriele GALATI, « CLS Bank et le risque de règlement dans les opérations de change », (2002) *Rapport trimestriel BRI* 1, 1-4.

59. Voir la sous-section suivante.

60. Le chèque doit être présenté par la banque d'encaissement dans un délai de 24 heures, selon la jurisprudence : *Stanley Works of Canada Ltd. c. Banque Canadienne Nationale*, [1982] R.L. 433 (C.A.); *Process Piping Specialties Inc. c. Banque canadienne impériale de commerce*, [1986] R.J.Q. 2429, EYB 1986- (à suivre...)

tances, ces délais peuvent s'étendre de trois à dix jours, mais pourront être plus longs pour un chèque provenant de l'extérieur du Québec, et surtout, du Canada. La période de retenue des fonds par la banque lors du dépôt d'un chèque est corrélée à ce délai⁶¹, sous réserve de certaines exceptions⁶². Une traite bancaire, réputée plus sécuritaire, exige un délai relativement court, moins de trois jours. Cependant, il faut garder à l'esprit les fraudes touchant certaines traites, notamment étrangères⁶³. L'article 16 du *Règlement sur la comptabilité en fidéicommiss des notaires* exige que le notaire dépose la somme reçue dans le compte en fidéicommiss dans un délai de trois jours⁶⁴. Or, le notaire doit patienter durant une période suffisante pour couvrir le délai de compensation à la suite de l'encais-

(...suite)

79020 (C.S.) (ces deux décisions de principe prévoyaient à l'époque un délai de 48 heures); la banque tirée qui retourne le chèque doit également le faire dans un délai de 24 heures : ASSOCIATION CANADIENNE DES PAIEMENTS (PAIEMENTS CANADA), *Règle A4 – Effets retournés et réacheminés*, 27 janvier 2020, art. 5, en ligne : <<https://www.paiements.ca/sites/default/files/a4fre.pdf>> [Règle A-4].

61. En vertu d'une disposition réglementaire, le délai de retenue d'un chèque ou autre effet d'au plus 1 500 \$, est de quatre jours ouvrables qui suivent la date du dépôt fait en personne auprès d'un employé de la succursale de l'institution ou d'un point de service, ou de cinq jours ouvrables qui suivent la date du dépôt, s'il a été fait de toute autre manière; dans le cas d'un chèque ou un autre effet de plus de 1 500 \$, le délai est de sept jours ouvrables qui suivent la date du dépôt fait en personne auprès d'un employé de la succursale de l'institution ou d'un point de service, ou de huit jours ouvrables qui suivent la date du dépôt, s'il a été fait de toute autre manière; une première tranche de 100 \$ est immédiatement disponible : *Règlement relatif à l'accès aux fonds*, DORS/2012-24, art. 3.
62. Notamment, lorsque : le compte de l'entreprise présente un découvert croissant qui n'est pas réduit par des dépôts; il y a eu une révision à la baisse de la cote de crédit ou d'autres cotes de comportement qui peuvent influencer le risque de crédit de l'entreprise; il s'est produit un changement inexpliqué dans l'historique des dépôts de chèques ou d'autres effets dans le compte; un nombre élevé de chèques ou d'autres effets déposés sont refusés par d'autres institutions, ce qui peut influencer sur le solde disponible du compte; l'entreprise fait l'objet d'un avis de faillite ou d'un avis de mesures prises par des créanciers; l'institution a des motifs raisonnables de croire que le chèque ou l'autre effet est déposé à des fins illégales ou frauduleuses relativement au compte du déposant; le compte est ouvert depuis moins de quatre-vingt-dix jours; le chèque ou l'autre effet a été endossé plus d'une fois; au moins six mois se sont écoulés depuis la date du chèque ou de l'autre effet : *Règlement relatif à l'accès aux fonds*, DORS/2012-24, art. 5-6. Un chèque provenant de l'étranger nécessite un délai beaucoup plus long, parfois jusqu'à 25 jours.
63. *Banque Nationale du Canada c. Bédard*, 2006 QCCS 5476, conf. par 2008 QCCA 539.
64. *Règlement sur la comptabilité en fidéicommiss des notaires*, RLRQ, c. N-3, r. 5.2.

sement d'un effet de commerce dans son compte en fidéicommiss avant l'utilisation des fonds⁶⁵.

À l'égard des effets de paiement papier qui transitent par le système de paiement, la banque tirée conserve le droit de les examiner avant la fin du jour ouvrable suivant. Le paiement devient définitif et irrévocable lorsque le paiement retourné par la banque tirée a été compensé.

Suivant la détermination du moment de l'achèvement du virement et les délais de compensation⁶⁶, une question fondamentale concerne la propriété des fonds. En principe, il est simple d'affirmer que lorsque le virement est achevé, la propriété des fonds change de patrimoine pour être transférée du donneur d'ordre au bénéficiaire. Or, cette question anodine en apparence est au cœur de l'arrêt *Compagnie d'assurances générales Co-Operators c. Coop fédérée*⁶⁷, dont la décision de la Cour d'appel a été portée devant la Cour suprême du Canada⁶⁸. En l'espèce, la Coop fédérée a été victime d'un stratagème d'hameçonnage. Elle a ordonné à son institution financière, la Banque Nationale du Canada, de transférer électroniquement la somme de 4 946 355,26 \$ US [5 415 179,81 \$ CA]⁶⁹ au compte du bénéficiaire désigné dans une banque de Hong-Kong, sous le prétexte de procéder à une offre publique d'achat. Brièvement, la contrôlease a reçu un faux courriel de son directeur, et après des vérifications d'usage, a ordonné le transfert de l'argent. Lorsque Coop fédérée s'est rendu compte de l'arnaque, il était malheureusement trop tard pour arrêter le transfert de fonds, car le virement avait été achevé. La Cour d'appel a affirmé que les fonds étaient la propriété de la banque⁷⁰. En effet, en vertu du principe selon lequel le dépôt d'argent dans un compte bancaire constitue un prêt à la banque, celle-ci devenait la débitrice de son client. L'argent étant un

65. Cela respecte les exigences réglementaires : *Règlement sur la comptabilité en fidéicommiss des notaires*, RLRQ, c. N-3, art. 27, al. 1(1°).

66. Sur cette question, voir la thèse suivante : Arthur OULAÏ, *Contribution à la recherche d'une harmonisation dans le traitement juridique des risques reliés aux transferts électroniques de fonds à caractère commercial*, Thèse (LL.D.), Université Laval, 2002, 563 p.

67. 2019 QCCA 1678.

68. *Compagnie d'assurance générale Co-Operators c. Sollio Groupe Coopératif*, 2020 CSC 41.

69. Taux de change de la Banque du Canada pour le 21 août 2014, date de la fraude : 1,09478 \$ CA / 1 \$ US.

70. *Compagnie d'assurances générales Co-Operators c. Coop fédérée*, 2019 QCCA 1678, par. 105-111.

bien fongible, il devient la propriété de la banque, qui est responsable de remettre une somme équivalente sur demande⁷¹. Comme le souligne la Cour d'appel, « [l]e contrat de prêt d'argent ainsi formé par le dépôt dans un compte bancaire est qualifié de contrat réel : il se crée par le décaissement des sommes »⁷². En revanche, dans le cas d'une marge de crédit, ou d'un compte à découvert, le solde peut être créditeur ou débiteur : dans le premier cas, la banque assume les risques de perte alors que dans le second cas, c'est le client qui assume ces risques. En l'espèce, la Coop fédérée s'était vue octroyer une marge de crédit de 100 000 000 \$ CA par la Banque Nationale du Canada. Le solde de ce compte, qui était débiteur de 3 386 361,80 \$ US, s'est accru d'une somme supplémentaire de 4 946 355,26 \$ US à la suite de la fraude, pour un total de 8 332 717,06 \$ US. À la suite de l'ordre de paiement soumis par la Coop fédérée à la Banque Nationale du Canada, la Coop fédérée était débitrice envers la banque du montant correspondant. Ainsi, la Coop fédérée était propriétaire de la somme d'argent volée⁷³.

1.2.2 Nouveaux développements

La compensation et le règlement interbancaires font l'objet de développements intéressants depuis quelques années, tant en ce qui a trait aux chèques (1.2.2.1) qu'aux transferts électroniques de fonds (1.2.2.2).

1.2.2.1 Chèque

Le processus de compensation d'un chèque a connu un virage technologique important en 2007 lorsque la *Loi sur les lettres de change* a été modifiée pour permettre qu'une image officielle d'un chèque ait la même valeur juridique qu'un effet papier⁷⁴. La raison

71. *Compagnie d'assurances générales Co-Operators c. Coop fédérée*, 2019 QCCA 1678, par. 108; art. 2327 C.c.Q.; Nicole L'HEUREUX et Marc LACOURSIÈRE, *Droit bancaire*, 5^e éd., Montréal, Éditions Yvon Blais, 2017, n^o 156, p. 121-122. Puisque la marge de crédit constitue une promesse de prêt, en vertu de l'art. 2316 C.c.Q. : *Compagnie d'assurances générales Co-Operators c. Coop fédérée*, 2019 QCCA 1678, par. 109.

72. *Compagnie d'assurances générales Co-Operators c. Coop fédérée*, 2019 QCCA 1678, par. 108.

73. *Compagnie d'assurances générales Co-Operators c. Coop fédérée*, 2019 QCCA 1678, par. 109-111.

74. *Loi sur les lettres de change*, L.R.C. (1985), ch. B-4, art. 163.1-163.8; ASSOCIATION CANADIENNE DES PAIEMENTS (PAIEMENTS CANADA), *Règle A10 – Règle d'imagerie*, 12 juillet 2019, en ligne : <<https://www.paiements.ca/sites/default/files/a10fre.pdf>> [Règle A10].

est de permettre à la banque d'encaissement de numériser le chèque, après son dépôt par le bénéficiaire, dans le but de faciliter et d'accélérer la compensation interbancaire. Conséquemment, les risques systémiques sont atténués, les délais de retenue des fonds sont abrégés et les risques de fraude et d'erreur sont réduits. Les clients ont également la possibilité de visionner leurs chèques par l'entremise d'Internet, ce qui augmente d'autant la qualité du service à la clientèle. Enfin, les délais de recherche d'un chèque numérisé sont plus rapides que pour un chèque papier.

Ainsi, depuis 2013⁷⁵, les institutions financières canadiennes permettent à leurs clients de déposer un chèque par téléphone intelligent, à l'aide d'une application conçue à cet effet. Très conviviale, cette opération, appelée « télésaisie du chèque » par Paiements Canada, peine toutefois à favoriser l'utilisation du chèque, comme en fait foi la diminution constante de son emploi par des consommateurs⁷⁶. D'une simplicité désarmante, l'opération consiste pour le consommateur à photographier le chèque (papier) et à le transmettre à son institution financière par l'application fournie par celle-ci. Le chèque doit être conservé quelques jours avant sa destruction. Les avantages sont certes bien intéressants, mais il subsiste le problème du dépôt double ou multiple⁷⁷.

Le dépôt numérique d'un chèque soulève un problème juridique qui peut s'avérer important. Le chèque est un document de titre, c'est-à-dire qu'il n'existe qu'un seul exemplaire original qui contient les droits des parties. Or, lors de la télésaisie du chèque, l'effet numérisé est déposé et l'original demeure dans les mains du client. Si, par mégarde ou sciemment, le client dépose le chèque original (papier) après l'avoir numérisé, les deux seront transmis à la compensation. Les cas sont rares, mais Paiements Canada prend au sérieux cette question. D'entrée de jeu, l'alinéa 5(1)b) de la *Loi cana-*

75. Benjamin GEVA, « Is the Death of the Paper Cheque Upon Us? The Electronic Presentment and Deposit of Cheques in Canada », (2015) 30 *B.F.L.R.* 113; Bradley CRAWFORD, *The Law of Banking and Payment in Canada*, Aurora (Ont.), Canada Law Book, 2008 (feuilles mobiles), n° 34:25.30(4), p. 34-18.2.

76. Nicole L'HEUREUX et Marc LACOURSIÈRE, *Droit bancaire*, 5^e éd., Montréal, Éditions Yvon Blais, 2017, n° 888, p. 671; *supra*, notes 1 et 6 et le texte correspondant.

77. Benjamin GEVA, « Is the Death of the Paper Cheque Upon Us? The Electronic Presentment and Deposit of Cheques in Canada », (2015) 30 *B.F.L.R.* 113, 120-122.

dienne sur les paiements n'interdit pas cette innovation⁷⁸. Paiements Canada croit que la Règle A4 est difficilement adaptable dans le contexte d'un chèque numérique⁷⁹. En effet, les articles 4(b) et 6(c) permettent à la banque tirée de retourner « l'effet de paiement en double », c'est-à-dire qui a été présenté deux fois au paiement⁸⁰. Le problème de la télésaisie vise plutôt le dépôt en double, ou double encaissement, par le bénéficiaire. Il n'est toutefois pas certain que le paragraphe 165(3) de la *Loi sur les lettres de change*⁸¹, concernant les droits et pouvoirs du détenteur régulier par la banque lors d'un dépôt, et l'article 163.1, qui a trait à la présentation au paiement par la banque d'encaissement de l'image officielle d'un chèque, puissent s'appliquer⁸².

Intuitivement, la banque tirée devrait être responsable des dépôts doubles ou multiples, car elle a proposé au client un environnement qui permet le dépôt d'un chèque de manière numérique⁸³. La banque tirée devrait, à tout le moins, pouvoir détecter les dépôts subséquents au premier dépôt, car après tout, elle doit connaître son client. Peut-elle s'exonérer d'une telle erreur ? L'exonération de la banque en cas de paiement malgré un contrordre est parfois

78. *Loi canadienne sur les paiements*, L.R.C. (1985), ch. C-21; Bradley CRAWFORD, *The Law of Banking and Payment in Canada*, Aurora (Ont.), Canada Law Book, 2008 (feuilles mobiles), n° 34:25.30(4), p. 34-182.

79. ASSOCIATION CANADIENNE DES PAIEMENTS (PAIEMENTS CANADA), *Règle A4 – Effets retournés et réacheminés*, 27 janvier 2020, art. 22(a), en ligne : <<https://www.paiements.ca/sites/default/files/a4fre.pdf>>.

80. L'article 2(c) définit l'« Effet de paiement en double » comme un « [e]ffet autorisé qui a été présenté au paiement plus d'une fois. Cela peut se produire lorsqu'un original et soit une image, un imprimé d'image ou une photocopie ont tous deux été présentés au paiement; que soit un effet original a été présenté au paiement plus d'une fois; ou que soit une image, un imprimé d'image ou une photocopie a été présenté au paiement plus d'une fois ».

81. L.R.C. (1985), ch. B-4.

82. Selon M^e Bradley Crawford, il serait possible de justifier l'application de cette disposition en vertu de la théorie de la « constructive delivery » (livraison par interprétation), qui se fonde sur la notion juridique du contrôle par une personne qui détient l'effet physique sur celle qui ne la détient pas, en vertu de l'arrêt *Watson c. Bradshaw*, (1881) 6 O.R. 666 (Ont. C.A.). Il ajoute toutefois que si le client n'est pas considéré comme le mandataire (*agent*) de la banque, l'image du chèque déposé par le consommateur ne peut se qualifier comme une image officielle au sens de l'article 163.1 ni de l'article 3(d) de la Règle A10 : Bradley CRAWFORD, *The Law of Banking and Payment in Canada*, Aurora (Ont.), Canada Law Book, 2008 (feuilles mobiles), n^{os} 34:25.30(4)-(4)(b), p. 34-18.2a-34-18.2i.

83. Benjamin GEVA, « Is the Death of the Paper Cheque Upon Us? The Electronic Presentment and Deposit of Cheques in Canada », (2015) 30 *B.F.L.R.* 113, 121-122.

acceptée⁸⁴ de même que l'exonération fondée sur l'accord de vérification. Or, si le client ne respecte pas la procédure à suivre, il se peut que cette exonération ne soit pas accordée⁸⁵.

Aux États-Unis, où les chèques sont plus usités qu'au Canada, une récente modification à la *Regulation CC*⁸⁶ tient la banque d'encaissement qui accepte la télésaisie, dont le chèque n'est pas endossé restrictivement, responsable vis-à-vis les autres banques, de même que vis-à-vis le tireur, l'incitant à plus de prudence, notamment adopter une politique et une procédure sécuritaires pour combattre la fraude ou émettre un avertissement dès que le dépôt d'une télésaisie (appelé *remote deposit capture*) a été effectué⁸⁷.

L'avantage d'un endossement restrictif, permis par l'article 67 de la *Loi sur les lettres de change*⁸⁸, repose sur l'idée que le bénéficiaire devrait indiquer à l'endos du chèque son nom, et le numéro du compte, où le chèque doit être déposé, ce qui empêche la négociation du chèque. De cette manière, il pourrait difficilement être déposé en double, car la banque d'encaissement pourrait alors constater le double lorsque le bénéficiaire dépose le chèque une seconde fois par l'entremise de son système informatique. Si les fonds étaient retenus systématiquement par la banque d'encaissement, cela empêcherait possiblement qu'un bénéficiaire le dépose de nouveau par mégarde, mais pas que le bénéficiaire mal intentionné le dépose une seconde fois plusieurs jours plus tard. Un chèque barré pourrait apporter une sécurité supplémentaire, empêchant la

84. Nicole L'HEUREUX et Marc LACOURSIÈRE, *Droit bancaire*, 5^e éd., Montréal, Éditions Yvon Blais, 2017, n^o 347, p. 244-245.

85. Voir *infra*, note 105 et le texte correspondant.

86. *Availability of Funds and Collection of Checks (Regulation CC)*, 12 CFR 229.34(f). Si, par hypothèse, le chèque est déposé une première fois par le bénéficiaire, il suit la pérégrination habituelle, c'est-à-dire qu'il est accepté par la banque tirée, retourné à la banque du bénéficiaire pour crédit définitif. Lors de la seconde tentative, le chèque est redéposé et est de nouveau transmis à la banque tirée qui devrait, en principe, le refuser. Si la banque du bénéficiaire décide de retenir les fonds sur tous les effets déposés par télésaisie, le risque diminue, mais n'est pas éliminé. En effet, une image pourrait être déposée en premier lieu, et pour le second dépôt, il s'agirait du chèque pallier, et à ce moment la banque du bénéficiaire pourrait n'avoir aucune raison de ne pas le retenir, et pourrait même invoquer son statut de détenteur régulier. Cette dernière situation pose un problème, et le droit américain tente d'y remédier.

87. *Taubman v. USAA Fed. Sav. Bank*, 408 F. Supp. 3d 1053, 1056-1057, 2019 U.S. Dist. LEXIS 175453, 2019 WL 4927116 (United States District Court, N.D., Ca.).

88. L.R.C. (1985), ch. B-4.

négociation à une tierce personne⁸⁹. Au demeurant, le tireur devrait également agir prudemment, et vérifier régulièrement ses relevés bancaires, notamment dans le site Internet de sa banque, comme le prévoient d'ailleurs les contrats bancaires⁹⁰.

Face à cette incertitude juridique, l'accent devrait être mis sur la prévention par les institutions financières et, plus généralement, sur le système financier canadien en général. Dans ces circonstances, nous approuvons la vision de M^e Bradley Crawford qui souligne qu'il serait peut-être plus judicieux pour une banque de limiter le montant à une somme relativement modeste qui peut être déposée par téléphone cellulaire, puisque certaines banques permettent actuellement le dépôt de sommes très substantielles⁹¹. Confronté à une exposition potentiellement plus importante des tireurs d'un chèque dans le contexte d'un dépôt numérique⁹², Paiements Canada s'est interrogé sur la possibilité pour les institutions financières d'utiliser un logiciel de détection des doubles, sur le délai de 90 jours de retour des effets de paiement en double, notamment en raison de l'expérience américaine, et sur l'adéquation de la *Loi sur les lettres de change*⁹³. En définitive, peut-être M^e Crawford a-t-il raison d'affirmer ce qui suit :

The technical, practical and policy difficulties raised by these new mobile phone image deposit facilities are impelling : this is an unsafe and unsound banking practice which should be prohibited before it causes confusion and disruption of the ACSS [SACR].⁹⁴

89. *Loi sur les lettres de change*, L.R.C. (1985), art. 168.

90. Voir *infra*, note 105 et le texte correspondant.

91. Bradley CRAWFORD, *The Law of Banking and Payment in Canada*, Aurora (Ont.), Canada Law Book, 2008 (feuilles mobiles), n° 34:25.30(4)(b), p. 34-18.2n.

92. PAIEMENTS CANADA, « L'ACP anime un dialogue de l'industrie sur les effets de paiement en double dans l'environnement d'imagerie (Effets en double, partie 1) », 18 février 2015, en ligne : <<https://www.paiements.ca/about-us/news/lacp-anime-un-dialogue-de-lindustrie-sur-les-effets-de-paiement-en-double-dans>>; PAIEMENTS CANADA, « Leçons tirées de l'expérience américaine (Effets en double, partie 2) », 2 mars 2015, en ligne : <<https://www.paiements.ca/à-propos/nouvelles/leçons-tirées-de-lexpérience-américaine-effets-en-double-partie-2>>; PAIEMENTS CANADA, « Le cadre canadien actuel (Effets en double, partie 3) », 30 mars 2015, en ligne : <<https://www.paiements.ca/à-propos/nouvelles/le-cadre-canadien-actuel-effets-en-double-partie-3>>; PAIEMENTS CANADA, « Qu'est-ce qui pourrait devoir changer dans l'environnement d'imagerie ? (Effets en double, partie 4) », 27 avril 2015, en ligne : <<https://www.paiements.ca/à-propos/nouvelles/quest-ce-qui-pourrait-devoir-changer-dans-lenvironnement-dimagerie-effets-en>>.

93. L.R.C. (1985), ch. B-4.

94. Bradley CRAWFORD, *The Law of Banking and Payment in Canada*, Aurora (Ont.), Canada Law Book, 2008 (feuilles mobiles), n° 34:25.30(4)(b), p. 34-18.2m.

Nonobstant ces innovations cambiaires, Paiements Canada mise sur les paiements électroniques pour le développement du système de paiement canadien.

1.2.2.2 Transfert électronique de fonds

En 2015, Paiements Canada a entrepris une révision en profondeur du système de paiement au Canada. L'année suivante, deux études ont évalué les besoins du marché canadien. D'abord, le document *Pour une vision commune pour l'écosystème de paiement canadien* vise la mise en œuvre d'un « système de paiement moderne qui est rapide, souple et sûr, favorise l'innovation et renforce la compétitivité du Canada »⁹⁵.

Par la suite, à partir de cette vision commune, Paiements Canada a publié la *Carte routière et le plan de haut niveau de l'industrie*, qui est destinée à mettre en œuvre la vision commune, c'est-à-dire de répondre aux besoins de l'industrie et à moderniser l'écosystème des paiements⁹⁶.

Enfin, l'*État cible de la modernisation* présente un portrait détaillé du programme de modernisation de Paiements Canada⁹⁷. Il

95. PAIEMENTS CANADA, *Pour une vision commune de l'écosystème de paiement canadien*, 21 avril 2016, en ligne : <https://www.paiements.ca/sites/default/files/vision-ecosysteme-paiements-canadien_edited_0.pdf> [Vision]. Concrètement, il s'agissait de recueillir des renseignements à partir de consultations, de définir le système de paiement, d'étudier les exigences des organismes de réglementation, d'évaluer le Système de transfert de paiements de grande valeur (STPGV), d'explorer les solutions disponibles pour un système de règlement de base et d'évaluer la technologie du grand livre distribué.

96. PAIEMENTS CANADA, *Carte routière et le plan de haut niveau de l'industrie*, décembre 2016, en ligne : <https://www.payments.ca/sites/default/files/paymentscanada_roadmapreader_fr.pdf>.

97. PAIEMENTS CANADA, *État cible de la modernisation : Résumé des principales exigences, de l'état final conceptuel, du plan de travail intégré et des avantages du programme de modernisation*, décembre 2017, en ligne : <https://www.payments.ca/sites/default/files/21-déc.-17/modernization_target_state_final_fr.pdf?_ga=2.137802680.96920963.1536767364-1201800425.1536767364> [État cible]. L'État cible décrit les systèmes modernisés et leurs structures de soutien fondamentales (cadres de risque et de réglementation, modèles d'accès), et présente l'état cible de la modernisation, l'intégration des systèmes modernes, la migration possible des types de paiements et les avantages escomptés pour les entreprises et les ménages canadiens. Voir également : MINISTÈRE DES FINANCES (CANADA), *Rapport sur l'examen de la Loi canadienne sur les paiements*, 2019, en ligne : <<https://www.canada.ca/content/dam/fin/migration/activty/consult/rcpa-elcp-report-rapport-fra.pdf>>.

focalise sur trois aspects : le remplacement du STPGV par une nouvelle structure, appelée Lynx, mieux adaptée aux normes de gestion du risque de la Banque du Canada; le remplacement du SACR par le Moteur d'optimisation du règlement (MOR), également mieux adapté aux normes de gestion du risque de la Banque du Canada; enfin, la mise en œuvre d'un nouveau système de paiement en temps réel (PTR). Dans ce dernier cas, Paiements Canada permettra aux fournisseurs de service de paiement de type non financier d'accéder directement au système de paiement en temps réel, avalisant ainsi l'approche préconisée par la Vision en avril 2016⁹⁸.

En d'autres termes, Paiements Canada procède à une modernisation majeure du système de paiement canadien en permettant, entre autres à des fournisseurs de service de paiement de type non financier, d'accéder au système de compensation interbancaire.

En ce qui a trait aux conséquences de ces mesures sur la pratique notariale, le MOR permet d'assurer un processus de compensation plus sécuritaire, mais demeure, somme toute, abstrait pour le notaire. Par contre, il pourrait diminuer les délais de compensation lors d'une transaction avec un sous-adhérent au système de compensation⁹⁹. Toutefois, le système de paiement en temps réel promet d'avoir une incidence positive sur la pratique notariale en raison de l'élimination du délai de compensation. Le système de paiement en temps réel constitue une « nouveauté pour le Canada », selon Paiements Canada¹⁰⁰. En activité 24 heures sur 24 et 7 jours sur 7, les fonds sont acheminés en temps réel par un mécanisme piloté par crédit pour les virements. La norme ISO 20022 sera également utilisée pour la transmission des données qui accompagnent le paiement, augmentant ainsi l'efficacité du virement¹⁰¹. Ces paiements peuvent comprendre des factures, des numéros d'identifica-

98. PAIEMENTS CANADA, Vision. Concrètement, il s'agissait de recueillir des renseignements à partir de consultations, de définir le système de paiement, d'étudier les exigences des organismes de réglementation, d'évaluer le STPGV, d'explorer les solutions disponibles pour un système de règlement de base et d'évaluer la technologie du grand livre distribué.

99. PAIEMENTS CANADA, préc., note 97, p. 25.

100. PAIEMENTS CANADA, préc., note 97, p. 20.

101. PAIEMENTS CANADA, préc., note 97, p. 20. Cette norme vise l'utilisation d'une messagerie universelle pour l'industrie des services financiers. À ce sujet, voir : PAIEMENTS CANADA, Centre de ressources ISO 20022, 2017, en ligne : <<https://www.paiements.ca/ressources/centre-de-ressources-iso-20022>>.

tion uniques et même des adresses URL. Le règlement se réalise en différé (24 h) ou en temps réel¹⁰².

L'architecture technique modulaire utilisée pour le système en temps réel offrira de « nouvelles fonctionnalités et de nouveaux services adaptés aux nouvelles mesures réglementaires, aux besoins du marché et à la demande pour un plus grand accès »¹⁰³. Un système de paiement en temps réel sous-entend que l'échange et la compensation sont instantanés et irrévocables, et surtout, que la gestion des risques est largement bonifiée.

Soulignons que les Canadiens ont rapidement adopté les paiements électroniques. Si Paiements Canada a modernisé la compensation des chèques au fil des dernières années, la nouvelle vision présentée en 2016 vise à quitter définitivement l'ère archaïque des paiements papier pour encourager un système de transfert électronique de fonds où les paiements sont idéalement traités en temps réel.

Cette nouvelle approche, conjuguée à la plateforme Assyst Paiement, est conçue sur mesure pour répondre aux besoins de la pratique notariale, et appelle à une réflexion quant à l'utilisation des méthodes de paiement actuellement utilisées dans ce contexte. Au demeurant, les erreurs et les comportements frauduleux sont également diminués en l'absence du chèque.

2. Erreurs et comportements frauduleux

Les erreurs et les comportements frauduleux préoccupent régulièrement et de diverses manières le milieu financier, notamment le secteur bancaire. Les conséquences sont sérieuses, en particulier lorsqu'un tiers est à l'origine d'un comportement frauduleux. Outre les erreurs commises par la banque ou son client, les mécanismes de paiement, traditionnels ou du dernier cri, sont instrumentalisés pour commettre des actes frauduleux, alors que le compte bancaire devient l'objet de cette même fraude. La discussion est canalisée vers les cas susceptibles d'intéresser la pratique notariale. Nous discutons en premier lieu du problème concernant le

102. PAIEMENTS CANADA, préc., note 97, p. 23-24.

103. PAIEMENTS CANADA, préc., note 97, p. 20.

paiement (2.1), pour ensuite analyser les circonstances touchant le compte en fidéicommiss (2.2).

2.1 Paiement

Comme souligné ci-dessus, les longs délais nécessaires à la compensation du chèque peuvent engendrer plusieurs problèmes, comme des erreurs, un contrordre, une faillite ou un comportement frauduleux. Aux fins de ce texte, nous focaliserons essentiellement sur ce dernier aspect (2.1.1). Or, les transferts électroniques de fonds ne sont pas à l'abri d'une erreur ou d'une fraude (2.1.2).

2.1.1 Chèque et traite bancaire

La fraude d'un chèque peut être commise par un employé d'une société qui a accès aux documents bancaires, qui travaille dans l'entreprise depuis plusieurs années et avec qui un climat de confiance s'est installé. Il s'agit d'un cas classique, souvent rapporté en jurisprudence. Bien que la falsification d'un chèque soit un phénomène très ancien et qu'elle soit bien encadrée en jurisprudence, elle suscite toujours des inquiétudes. La fraude d'un chèque tire son origine d'une fausse signature, d'un montant ou d'une date altérés, d'un faux endossement ou encore d'une combinaison de ces actions (2.1.1.1). D'autres situations prennent assise sur le délai de compensation (2.1.1.2).

2.1.1.1 Falsification de l'effet

En général, le stratagème de fraude se résume à falsifier la signature du tireur (signataire) d'un chèque (2.1.1.1.1) ou l'endossement (2.1.1.1.2). Parfois, la fraude est plus sophistiquée et combine la falsification de la signature du tireur et l'endossement de l'effet.

2.1.1.1.1 Falsification de la signature

En vertu de l'article 16 de la *Loi sur les lettres de change*¹⁰⁴, le chèque doit porter la signature du tireur. Il est présumé être authentique et autorisé. En cas de falsification, l'article 48 prévoit que le tireur n'est pas lié par le chèque, car la banque a l'obligation de vérifier l'authenticité de la signature de son client.

104. L.R.C. (1985), ch. B-4.

La reconnaissance de la signature du tireur est donc difficile en pratique et une contre-vérification par un caissier avec le carton de signature du tireur est pour le moins fastidieux. Conséquemment, les banques vérifient rarement les signatures. Elles ont conçu des clauses exonératoires qui ont été validées par les tribunaux depuis plus de 100 ans, lorsqu'elles sont claires et non ambiguës, ce qui est habituellement le cas de nos jours, celles-ci ayant été raffinées au fil des ans¹⁰⁵. Ces clauses prévoient que le client doit vérifier ses états bancaires et aviser la banque, dans un délai déterminé, de toute erreur ou anomalie¹⁰⁶.

2.1.1.1.2 Endossement frauduleux

L'endossement d'un chèque peut prendre deux formes : soit un chèque endossé seulement par le bénéficiaire, qui dépose le chèque directement à la banque d'encaissement, soit un chèque portant plus d'un endossement (habituellement deux, appelé « double endossement »), c'est-à-dire que le bénéficiaire a négocié le chèque à une autre personne (appelée « endossataire »), qui endossera à son tour le chèque et qui en deviendra le détenteur. C'est lui qui le déposera par la suite à la banque d'encaissement. Dans ce contexte, quelle est l'obligation de la banque d'encaissement ? À l'instar de la banque tirée, la banque d'encaissement a l'obligation de vérifier l'identité du bénéficiaire qui désire encaisser un chèque. Comment se manifeste cette vérification ? Quelles sont les obligations de la banque d'encaissement ?

La jurisprudence est particulièrement limpide sur cet aspect. Dans l'arrêt *Aird c. Banque Royale du Canada*¹⁰⁷, la Cour d'appel du Québec s'est penchée sur le cas d'une fraude commise par un mandataire à l'endroit d'une bénéficiaire d'une police d'assurance, en en falsifiant l'endossement. Après avoir constaté l'inaction de la banque d'encaissement face à des signaux importants, dont 29 contrordres de paiement et un chèque sans provision dans le compte du mandataire, la Cour a indiqué que la banque d'encaissement avait le

105. *Arrow Transfer Company Ltd. c. Banque Royale du Canada*, [1972] R.C.S. 845; *Société hôtelière Canadien Pacifique Ltée c. Banque de Montréal*, [1987] 1 R.C.S. 711; *Bernatchez c. Banque Royale du Canada*, [1999] R.R.A. 503 (C.S.); *Les Productions Mark Blandford Inc. c. Caisse populaire St-Louis de France*, [2000] R.J.Q. 1697 (C.A.); *9075-0878 Québec Inc. c. Banque Toronto Dominion*, 2006 QCCQ 9806.

106. Le délai est de 30 ou de 45 jours selon les contrats, mais il peut être moindre pour les clients commerciaux.

107. [1999] R.J.Q. 321 (C.A.).

devoir de vérifier l'endossement d'un chèque, surtout lorsque le déposant (endosseur) n'est pas le bénéficiaire. La Cour indique que « si l'institution bancaire décide de s'en remettre strictement à la réputation de son client, la victime, qui est une tierce partie quant à la négociation de l'effet de commerce [chèque], ne doit pas se trouver à en subir les préjudices »¹⁰⁸.

La bénéficiaire, qui était une tierce personne, a pu obtenir gain de cause par la voie d'un recours extracontractuel.

Cette décision de principe a contribué à l'amélioration des pratiques des banques d'encaissement au fil des ans¹⁰⁹. Concrètement, les banques sont devenues plus frileuses au regard des endossements provenant d'un chèque ayant été préalablement négocié par le bénéficiaire (double endossement). Elles refusent régulièrement le dépôt de ce type de chèque, à moins d'avoir pu effectuer une vérification auprès des parties impliquées. Ainsi, la banque d'encaissement ne peut payer un chèque sans avoir préalablement procédé à une enquête. Puisqu'elle est considérée comme une spécialiste des services bancaires, agir autrement constitue une conduite imprudente et négligente, bien que la bonne foi ne soit pas remise en cause. Il en résulte alors un préjudice pour le détenteur (endosseur)¹¹⁰.

Dans certains cas, une fraude cambiaire peut résulter de la combinaison de la falsification de la signature du tireur et de l'endossement. La falsification de la signature du chèque peut être l'œuvre du fraudeur lui-même, ou le fraudeur peut simplement convaincre le responsable de l'entreprise (autorisé à signer les chèques) qu'il doit payer un bénéficiaire en particulier (fournisseur actuel ou ancien, ou une personne dont le nom s'apparente à un fournisseur de l'entreprise). Lorsqu'il déposera le chèque, le fraudeur pourra falsifier l'endossement pour déposer le chèque dans son compte de banque personnel. Dans ce cas, il faut d'abord déterminer si la banque a commis un délit de détournement de fonds à l'égard du tireur du chèque, cette faute de common law s'appa-

108. *Aird c. Banque Royale du Canada*, [1999] R.J.Q. 321 (C.A.), p. 326.

109. Voir également : *Banque de Montréal c. Legault*, 2003 CanLII 20598 (QC C.A.). En doctrine, voir : Marc LEMIEUX, « La responsabilité résultant de l'encaissement et du paiement d'un chèque frauduleux », dans Service de la formation permanente, Barreau du Québec, vol. 195, *Développements récents en droit bancaire* (2003), Montréal, Édition Yvon Blais, 2003, p. 59.

110. *Aird c. Banque Royale du Canada*, [1999] R.J.Q. 321 (C.A.); *Banque de Montréal c. Legault*, 2003 CanLII 20598 (QC C.A.).

rentant à une responsabilité extracontractuelle¹¹¹. En effet, si le tireur a un lien de droit avec sa propre institution financière, la banque tirée, il n'existe cependant aucun lien de droit entre le tireur et la banque d'encaissement, celle-ci étant la banque du bénéficiaire. Ensuite, la banque d'encaissement pourra présenter une défense en vertu du paragraphe 20(5) de la *Loi sur les lettres de change*, appelée défense du bénéficiaire fictif. Cette disposition prévoit que, lorsque le chèque est destiné à un bénéficiaire qui est fictif ou qui n'existe pas, le chèque peut être considéré comme étant payable au porteur. Le cas échéant, la banque d'encaissement ne peut vérifier l'endossement car il n'est fait à l'ordre de personne. Concrètement, lors d'une fraude commise par un employé de l'employeur-tireur, le bénéficiaire ultime du chèque falsifié est le fraudeur lui-même. La *Loi sur les lettres de change*¹¹² est parsemée de mystères et le paragraphe 20(5) n'y fait pas exception¹¹³.

111. Tant pour les accords de vérification que pour les recours pour détournement (et vérification inadéquate de l'endossement), les règles de common law sont similaires à celles du droit civil.

112. L.R.C. (1985), ch. B-4.

113. Voir à ce sujet : *Banque Royale du Canada c. Concrete Column Clamps (1961) Ltd.*, [1977] 2 R.C.S. 456; *Boma Manufacturing Ltd. c. Banque Canadienne Impériale de Commerce*, [1996] 3 R.C.S. 727; et *Teva Canada Ltée c. TD Canada Trust*, 2017 CSC 51. La qualification d'un bénéficiaire fictif ou inexistant est suffisamment complexe pour avoir été analysée par la Cour suprême du Canada à quelques reprises. Est-ce que le tireur avait l'intention d'avantager le bénéficiaire ? Sinon, il est considéré comme un bénéficiaire fictif, et la banque d'encaissement n'a pas l'obligation de vérifier l'endossement, car le chèque est présumé au porteur (et non à l'ordre d'un bénéficiaire). Dans le cas contraire, le tireur voulait réellement payer le bénéficiaire, et ce dernier n'étant pas fictif, le chèque est considéré comme ayant été tiré à l'ordre de ce bénéficiaire et la banque d'encaissement doit vérifier l'endossement. Le débat jurisprudentiel prend sa source dans la détermination de l'intention du tireur : doit-on considérer le tireur comme l'âme dirigeante de la société, ou comme le signataire ? Doit-on considérer l'intention (élément subjectif), ou le simple fait que la société ait une créance à faire valoir contre le bénéficiaire (élément objectif) ? Dans les arrêts *Banque Royale du Canada c. Concrete Column Clamps (1961) Ltd.*, *Boma Manufacturing Ltd. c. Banque Canadienne Impériale de Commerce* et *Teva Canada Ltée c. TD Canada Trust*, la Cour suprême a retenu que l'intention du tireur (employeur) du chèque était déterminante, et non celle du signataire (le fraudeur). Ce point de vue constitue l'état actuel du droit, malgré sa controverse. Il est intéressant de conclure cette sous-section sur les arguments des juges La Forest et Abella. D'abord, le juge La Forest, dissident dans l'arrêt *Boma*, mentionnait que l'employeur tireur était le mieux placé que la banque pour empêcher les gestes de l'employeur fraudeur. Ensuite, la juge Abella, s'exprimant pour la majorité dans l'arrêt *Teva*, souligne que « [l]es banques sont bien placées pour gérer les pertes infligées par un chèque (à suivre...) »

2.1.1.2 Fraudes et délais de compensation

Le délai de compensation interbancaire d'un chèque et d'une traite bancaire est particulièrement propice aux comportements négligents et frauduleux. D'abord, durant le délai de compensation, le tireur d'un chèque peut révoquer son ordre de paiement¹¹⁴ ou éprouver des difficultés financières, que ce soit l'insolvabilité ou la faillite¹¹⁵. Ensuite, lorsqu'un chèque est déposé, la banque d'encaissement peut retenir les fonds pour la durée de la compensation ou accorder l'accès aux fonds. Les banques peuvent retenir les fonds d'un chèque ou d'une traite bancaire, sauf un minimum de 100 \$ ou plus, selon le contrat bancaire, et sauf dans quelques circonstances particulières¹¹⁶. Or, en pratique, les banques désirent répondre aux besoins de leurs clients et, selon que certains critères soient remplis, ne retiennent pas les fonds : l'historique du déposant, le solde moyen au compte du client, la durée de la relation du client avec la succursale, la valeur de l'effet, les lignes directrices internes de la banque, le moment du dépôt, le type de chèque (ou de traite) et une activité inusitée au compte. En cas de non-retenue de fonds, la banque d'encaissement octroie un crédit temporaire durant le délai de compensation, lequel deviendra définitif lorsque la pérégrination du chèque sera achevée. Ce délai de quelques jours est délicat, car, d'une part, il favorise les fraudes qui surviennent sous divers aspects¹¹⁷ et, d'autre part, la responsabilité de la banque peut être engagée.

(...suite)

frauduleux, car elles peuvent les répartir entre les utilisateurs au lieu d'exposer à la faillite les particuliers ou les petites entreprises victimes de la fraude » : par. 67. Selon nous, l'argument fondé sur le pouvoir économique des banques (*deep pocket policy*) ne devrait pas être retenu pour tenir une banque responsable.

114. *Loi sur les lettres de change*, L.R.C. (1985), ch. B-4, art. 167a).

115. Voir notamment : *Stanley Works of Canada Ltd. c. Banque Canadienne Nationale et Banque Royale*, [1982] R.L. 433 (C.A.); *National Slag c. Canadian Imperial Bank of Commerce*, (1982) 140 D.L.R. (3d) 473 (Ont. H.C.), conf. par (1985) 19 D.L.R. (4th) 383 (C.A.); *Midland Doherty Limited c. The Royal Bank of Canada*, [1990] R.J.Q. 121 (C.A.); *Process Piping Specialities Inc. c. La Banque Canadienne Nationale du Canada*, [1986] R.J.Q. 2429 (C.S.); *Banque Nationale du Canada c. Caisse centrale Desjardins du Québec*, [2001] R.J.Q. 846 (C.A.); *B.M.P. Global Distribution Inc. c. Banque de Nouvelle-Écosse*, 2009 CSC 15.

116. Voir *supra*, notes 61-63 et le texte correspondant.

117. En outre, nous pouvons ajouter le cas de la cavalerie de chèques, qui consiste en un stratagème de détournement de fonds qui repose sur des fonds fictifs et les délais de compensation. À ce sujet, voir : *Location Bristar Idealease Inc. (Syndic de)*, 2012 QCCS 211.

Habituellement, un fraudeur pourra ordonner un transfert électronique de fonds durant la compensation du chèque, ce dernier pouvant revenir sans provision. En pratique, cette situation se produit lorsque le fraudeur convainc une personne d'accepter de déposer un chèque, étant substantiellement rémunérée pour ce service, et de rapidement ordonner le transfert de fonds à un bénéficiaire, parfois situé à l'étranger. Concrètement, il s'agit d'une opération de blanchiment d'argent. L'arrêt *Banque Nationale du Canada c. Bédard* illustre cette fraude¹¹⁸. En l'espèce, le défendeur avait reçu une traite bancaire de 1,5 M\$ US du Zimbabwe, et l'avait déposé à une succursale de la Banque Nationale du Canada, située à Québec. La banque n'avait pas retenu les fonds de la traite. Après avoir constaté que la traite était frauduleuse, la banque n'a récupéré qu'une partie des fonds. Puisque la traite avait été déposée quelques minutes avant la fermeture du comptoir de la banque, que le montant était très élevé par rapport aux activités habituelles du client, qu'elle provenait d'un pays étranger et que le client aurait accepté que la banque retienne les fonds durant quelques jours, la Cour supérieure a considéré que la préposée de la banque a commis une négligence grave en acceptant le dépôt de cette traite, et qu'elle a donné au client « un faux sentiment de sécurité en lui indiquant que les fonds étaient immédiatement disponibles »¹¹⁹, ce qui a été confirmé en appel¹²⁰. Cette décision a eu un effet important sur le traitement des traites bancaires, lesquelles étaient toujours apparus très sécuritaires.

2.1.2 Transferts électroniques de fonds

Si le délai de compensation est habituellement rarement mis en cause dans le cas d'un effet de commerce, la question de l'identification du client devient centrale au virement bancaire. En effet, l'obligation de la banque du donneur d'ordre et celle de la banque du bénéficiaire partagent un point commun, soit la vérification de l'identité de leur client, peu importe qu'il s'agisse de décisions plus anciennes¹²¹ ou récentes¹²². Les décisions canadiennes sur cette question ne sont pas légion, ce qui peut témoigner de la fiabilité des

118. *Banque Nationale du Canada c. Bédard*, 2006 QCCS 5476, conf. par 2008 QCCA 539.

119. *Banque Nationale du Canada c. Bédard*, 2006 QCCS 5476, conf. par 2008 QCCA 539, par. 86, 101.

120. *Banque Nationale du Canada c. Bédard*, 2006 QCCS 5476, conf. par 2008 QCCA 539.

121. *Royal Bank of Canada c. Stangl*, [1992] O.J. No. 378 (Div. Gén. Ont.).

122. *Compagnie d'assurances générales Co-Operators c. Coop fédérée*, 2019 QCCA 1678.

transports électroniques de fonds, contrairement au cortège de décisions concernant les effets de commerce. Or, les nouvelles technologies ont ouvert la porte à des piratages commis par des tiers (2.1.2.2). Cette tendance récente ne doit pas faire oublier le comportement frauduleux d'un employé ou d'un dirigeant de l'institution financière (2.1.2.1).

2.1.2.1 Fraude interne

Le 20 juin 2019, la population québécoise a appris avec stupéfaction que la plus grande institution financière de la province, le Mouvement Desjardins (Desjardins), avait été victime d'une fraude commise par un employé¹²³. Les mois qui ont suivi ont permis de comprendre l'ampleur du désastre, car tous les membres de Desjardins ont été touchés¹²⁴. Ironiquement, l'onde de choc pourrait se ressentir d'une manière positive, non seulement en sensibilisant la population, mais surtout le législateur, comme en fait foi une déclaration de la ministre de la Justice du Québec et le dépôt de deux projets de loi¹²⁵ au sujet de la modernisation et du renforcement législatif de la protection des renseignements personnels¹²⁶. Essentiellement, un employé malintentionné a copié des informations personnelles des membres sur trois clés USB, pour les revendre par la suite. Il est donc établi qu'un vol de données personnelles a eu lieu, ouvrant la voie à des vols d'identité susceptibles de donner lieu à des conséquences financières pour les victimes¹²⁷. Desjardins a agi

123. Vincent LAROUCHE, « Les renseignements de 2,9 millions de membres de Desjardins dérobés », *La Presse*, 20 juin 2019, section Affaires.

124. Un total de 4,2 millions de membres ont été touchés, en plus de 1,8 million de détenteurs de cartes de crédit : Tristan PÉLOQUIN et Hugo PILON-LAROSE, « Fuite de données : tous les membres particuliers de Desjardins sont victimes », *La Presse*, 1^{er} novembre 2019, section Affaires. Voir également, au sujet d'une fraude visant Capital One : Luc OLINGA, « Capital One : vol des données de millions de clients, dont 6 millions de Canadiens », *La Presse*, 29 juillet 2019, section Affaires; Rob MCLEAN, « A Hacker Gained Access to 100 Million Capital One Credit Card Applications and Accounts », *CNN Business*, 30 juin 2019.

125. *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*, projet de loi n° 64 (adoption du principe – 20 octobre 2020), 1^{re} sess., 42^e légis. (Qc); *Loi sur les agences de crédit*, projet de loi n° 53 (adoption – 22 octobre 2020), 1^{re} sess., 42^e légis. (Qc).

126. Fanny LÉVESQUE, « Données personnelles: une loi avec plus de mordant », *La Presse+*, 12 février 2020, section Actualités, écran 2; Laura-Julie PERREAULT, « Sortir les dents », *La Presse+*, 24 février 2020, section Débats, écran 2. La question des renseignements personnels dépasse le cadre de ce texte, nous n'élaborons pas davantage à ce sujet.

127. *Langlois c. Fédération des caisses Desjardins du Québec*, 2021 QCCS 1; *Lemoine c. Fédération des caisses Desjardins du Québec*, 2021 QCCS 1135; (à suivre...)

rapidement en offrant gratuitement un service de protection d'une durée de cinq ans de l'agence de crédit Equifax, en plus de couvrir les pertes éventuelles (50 000 \$) et de former un comité pour analyser la situation. Cette fraude est rapidement devenue un cas d'école. Plusieurs questions demeurent en suspens, notamment l'étendue de la responsabilité de Desjardins.

Puisque Desjardins et ses membres sont les victimes d'une arnaque à l'interne, les sages paroles du juge La Forest, exprimées en dissidence dans l'arrêt *Boma* en 1996, doivent être considérées par les clients des banques¹²⁸, c'est-à-dire en l'espèce, le notaire. Le juge La Forest affirmait en effet qu'entre ces deux victimes innocentes, l'employeur devait assumer la responsabilité des gestes posés par son employé fautif, car il est le mieux placé pour prévenir cette fraude. Si, par hypothèse, une fraude financière est commise par l'employé d'un notaire, il n'est pas exclu que ce dernier soit tenu responsable.

La jurisprudence est très discrète sur cette question, mais l'affaire *Stangl* offre une piste de solution¹²⁹. En l'espèce, un virement bancaire, provenant de la Guyane vers une banque ontarienne (Banque Royale du Canada [RBC]), a été transmis par celle-ci à la banque du bénéficiaire (Banque Toronto Dominion [Banque TD]), laquelle l'a crédité dans le mauvais compte. La Banque TD a refusé de corriger l'erreur, contrairement aux usages bancaires en pareilles circonstances. Le commis de la Banque TD, responsable des virements, avait craint pour sa sécurité à la suite de menaces de voies de fait reçues de la part du bénéficiaire qui s'était vu créditer le montant par erreur (Joseph Stangl, président de Unitec). La Cour de justice de l'Ontario (division générale) a condamné la Banque TD à rembourser la RBC. Elle a par la suite condamné la défenderesse en garantie, Unitec, à rembourser la Banque TD.

2.1.2.2 Fraude d'un tiers

Les fraudeurs sont très imaginatifs et ne cessent de raffiner leurs supercheries bancaires, stimulés par les nouvelles technologies : fraudes de cartes de crédit, qui se déclinent en une multitude

(...suite)

Boulay c. Fédération des caisses Desjardins du Québec, Québec, n° 200-06-000231-194, 20 juin 2019.

128. Voir *infra*, notes 183 et 184 et le texte correspondant.

129. *Royal Bank of Canada v. Stangl*, [1992] O.J. No. 378 (Div. Gén. Ont.).

de variantes sur un même thème (clonage, etc.), fraudes de cartes de débit¹³⁰, virements par un téléphone cellulaire. Les fraudes visant les transferts électroniques de fonds sont toutefois plus susceptibles d'inquiéter le notaire.

Les délais de compensation et de règlement des paiements, épineux au pied des effets de commerce, soulèvent moins de contrariétés lorsqu'il est question de transferts électroniques de fonds, puisque dans ce dernier cas, ces délais sont très courts, sinon absents, et le droit de révocation est habituellement illusoire, sinon interdit.

Néanmoins, l'identification d'un client, qui participe à l'obligation des banques du donneur d'ordre et du bénéficiaire, est d'autant plus difficile que les fraudes technologiques se raffinent sans cesse. Deux affaires importantes, *M'Boutchou c. Banque de Montréal*¹³¹ et *Compagnie d'assurances générales Co-Operators c. Coop fédérée*¹³², en témoignent. Comme le souligne à juste titre le juge Jean-Yves Lalonde dans la décision *M'Boutchou c. Banque de Montréal*¹³³, « les transactions à distance par messages génèrent un facteur de risque plutôt élevé qui commande aux banques une obligation de prudence et de diligence accrue »¹³⁴.

L'affaire *M'Boutchou* constitue une décision de principe en matière de transferts électroniques de fonds. Dans cette affaire, monsieur Raphael M'Boutchou, citoyen canadien d'origine gabonaise, se déplace régulièrement au Canada pour ses affaires et sa famille. En septembre 2005, il ouvre deux comptes bancaires à la Banque de Montréal (« BMO » ou « la banque »), soit un compte courant et un compte d'épargne. Lors de l'ouverture de ce dernier compte, il y dépose la somme de 178 000 \$. Il effectue par la suite plusieurs transactions dans ses comptes. La banque reçoit par télécopieur une première demande de virement de fonds au profit d'un bénéficiaire thaïlandais le 14 novembre 2005, qu'elle décline pour absence d'autorisation écrite du demandeur. Le fraudeur (donneur

130. Sur cette question, voir généralement : Marc LACOURSIÈRE, « Propositions de réforme pour une protection des titulaires de cartes de débit victimes de transferts de fonds non autorisés », (2009) 54 R.D. McGill 91.

131. 2008 QCCS 5561.

132. 2019 QCCA 1678.

133. 2008 QCCS 5561.

134. *M'Boutchou c. Banque de Montréal*, 2008 QCCS 5561, par. 53.

d'ordre) récidive le 1^{er} décembre suivant en demandant à la banque, par téléphone, de lui faire parvenir une copie de ce formulaire afin qu'il le signe et le retourne. La banque donne suite à cette requête et reçoit quelques jours plus tard une deuxième demande de transfert électronique de fonds de 60 000 \$, laquelle est traitée le lendemain matin. La signature apparaissant sur le formulaire semble être celle du demandeur. Il appert que la vérification fut somme toute sommaire, puisqu'il n'y a eu que la comparaison des signatures avec les photocopies du passeport et du permis de conduire de monsieur M'Boutchou. La banque communique à l'étranger avec le signataire, qu'elle croit être monsieur M'Boutchou, et lui pose des questions à caractère personnel pour confirmer le tout. Or, le 6 décembre, soit au moment de l'envoi du formulaire, le demandeur n'était pas à l'étranger, mais bel et bien à Montréal pour effectuer un retrait au guichet automatisé de la banque, et en succursale le lendemain pour effectuer deux opérations de paiement.

La Cour supérieure donne raison au demandeur. La question au cœur du litige concerne le protocole d'autorisation que doit suivre la banque qui reçoit une demande de virement de fonds d'un client. Transposé à une opération notariale, ce protocole est au centre du partage de responsabilité entre le notaire et la banque dans le cas d'une fraude.

Quelle est l'intensité de l'obligation de la banque ? Au départ, un protocole doit être suivi pour identifier et authentifier le donneur d'ordre. Un point de départ repose sur les *Lignes directrices en matière d'identification et d'authentification* énoncées par le Commissariat à la protection de la vie privée du Canada (« Commissariat ») afin de prévenir l'usurpation d'identité¹³⁵. Ces lignes directrices, proposées conformément à la *Loi sur la protection des renseignements personnels et les documents électroniques*¹³⁶, indiquent que trois facteurs doivent être considérés : quelque chose que la personne connaît (par exemple, un mot de passe, un numéro d'identification personnel ou NIP, un numéro de compte, une couleur préférée, le nom du premier animal de compagnie), quelque chose que la personne possède (par exemple, une carte bancaire, un jeton

135. COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Lignes directrices en matière d'identification et d'authentification*, juin 2016, en ligne : <https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/identites/identification-et-authentification/auth_061013/>.

136. L.C. 2000, ch. 5, art. 5 et annexe 1.

d'authentification, une carte d'identité, un certificat d'utilisateur numérisé), et quelque chose qui fait partie de la personne (par exemple, un trait biométrique comme son visage, sa rétine ou sa voix) ou que seule *cette personne* peut faire (comme sa signature)¹³⁷.

Dans une optique de gestion du risque, le nombre de facteurs requis est corrélé à la sensibilité des informations. En ce qui concerne les renseignements financiers, considérés sensibles, le Commissariat à la vie privée note qu'« un processus d'authentification multicouches ou à plusieurs facteurs peut être requis pour les services financiers permettant de donner des instructions de paiement et d'effectuer des transferts à l'intention de tierces parties »¹³⁸.

Ces lignes directrices s'inspirent de la Directive révisée sur les paiements, adoptée par l'Union européenne en 2015¹³⁹. Cette directive est basée sur le concept de l'authentification forte du client. Selon l'article 74(2), si « le prestataire de services de paiement [banque] du payeur [donneur d'ordre] n'exige pas une authentification forte du client, le payeur ne supporte aucune perte financière », et si « le bénéficiaire ou son prestataire de services de paiement n'accepte pas une authentification forte du client, il rembourse le préjudice financier causé au prestataire de services de paiement du payeur ». Cette autorisation forte s'applique pour accéder à un compte de paiement, pour amorcer une opération de paiement ou

137. COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Lignes directrices en matière d'identification et d'authentification*, juin 2016, en ligne : <https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/identites/identification-et-authentification/auth_061013/>.

138. COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Lignes directrices en matière d'identification et d'authentification*, juin 2016, en ligne : <https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/identites/identification-et-authentification/auth_061013/>.

139. *Directive (UE) 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur, modifiant les directives 2002/65/CE, 2009/110/CE et 2013/36/UE et le règlement (UE) n° 1093/2010, et abrogeant la directive 2007/64/CE*, [2015] J.O. L337/35, art. 2(30) : « "authentification forte du client", une authentification reposant sur l'utilisation de deux éléments ou plus appartenant aux catégories "connaissance" (quelque chose que seul l'utilisateur connaît), "possession" (quelque chose que seul l'utilisateur possède) et "inhérence" (quelque chose que l'utilisateur est) et indépendants en ce sens que la compromission de l'un ne remet pas en question la fiabilité des autres, et qui est conçue de manière à protéger la confidentialité des données d'authentification ».

pour exécuter une action qui est susceptible de comporter un risque de fraude¹⁴⁰.

Il est également intéressant de souligner que le droit américain oblige la banque à utiliser une procédure de sécurité « commercialement raisonnable » pour contrer les transferts de fonds non autorisés¹⁴¹. Plus précisément, les mesures suivies par la banque doivent dépasser la simple comparaison de signatures, laquelle ne constitue pas en soi une procédure de sécurité. Les méthodes que doit utiliser la banque sont les mots d'identification, le cryptage de données ou, encore, le rappel téléphonique (ce qui consiste en une forme de reconnaissance vocale utilisée par la banque). Sur ce dernier point, il faut noter que l'article 5(e)(2)(v) de la *Règle H1 – Débits préautorisés (DPA)*, indique que « l'utilisation de méthodes biométriques comme la reconnaissance de la voix » est jugée comme étant commercialement raisonnable, reconnaissant ainsi implicitement que les développements technologiques permettent maintenant de rehausser le standard de vérification de l'identité du donneur d'ordre d'un virement de fonds¹⁴².

140. *Directive (UE) 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur, modifiant les directives 2002/65/CE, 2009/110/CE et 2013/36/UE et le règlement (UE) n° 1093/2010, et abrogeant la directive 2007/64/CE*, [2015] J.O. L337/35, art. 97(1). L'article 98 prévoit que les normes techniques sont développées par l'Autorité bancaire européenne : *Règlement délégué (UE) 2018/389 de la Commission du 27 novembre 2017 complétant la directive (UE) 2015/2366 du Parlement européen et du Conseil par des normes techniques de réglementation relatives à l'authentification forte du client et à des normes ouvertes communes et sécurisées de communication*, [2018] J.O. L69/23.

141. *Uniform Commercial Code*, Sect. 4A-202(b). Le paragraphe (c) de cette disposition précise que ce concept est une question de droit qui doit être déterminée par « the wishes of the customer expressed to the bank, the circumstances of the customer known to the bank, including the size, type, and frequency of payment orders normally issued by the customer to the bank, alternative security procedures offered to the customer, and security procedures in general use by customers and receiving banks similarly situated ».

142. ASSOCIATION CANADIENNE DES PAIEMENTS (PAIEMENTS CANADA), *Règle H1 – Débits préautorisés (DPA)*, 30 janvier 2017, en ligne : <<https://www.paiements.ca/sites/default/files/h1fre.pdf>>. Plus généralement, il est intéressant de souligner quelques circonstances et illustrations de méthodes jugées commercialement raisonnables, par l'article 5(1) de cette règle :

- i. la nature de l'entreprise particulière;
- ii. le montant de l'opération particulière;
- iii. le volume de paiements du bénéficiaire;
- iv. le niveau de connaissances techniques des parties;
- v. la disponibilité d'autres solutions offertes à l'une des parties mais rejetées par elle;

(à suivre...)

Dans l'affaire *M'Boutchou*, le comportement de la banque semble à première vue respecter les lignes directrices du Commissariat, puisque la préposée a vérifié les documents personnels et les signatures du client et qu'elle lui a posé des questions à caractère personnel (croyant à tort qu'il s'agissait du demandeur). Toutefois, il n'y a rien dans la décision qui indique que le demandeur effectuait régulièrement ses opérations en personne ou par téléphone. Le protocole n'a pas été suivi, et aucune vérification des transactions survenues dans le compte en banque du client n'est exigée et rien ne permet de s'assurer que le bénéficiaire soit bien identifié¹⁴³.

Dans la décision *Compagnie d'assurances générales Co-Operators c. Coop fédérée*¹⁴⁴, la Cour d'appel ne s'est attardée ni au comportement du donneur d'ordre, en l'espèce la Coop fédérée, ni à la dimension sécuritaire intrinsèque à ce genre de transactions. Bien que l'arrêt soit fondé en droit, il eut été intéressant qu'on y aborde la question du partage de responsabilité entre le donneur d'ordre et sa banque, soit la Banque Nationale du Canada. La Cour considère d'abord que ces parties sont les victimes d'une arnaque savamment orchestrée, pour ensuite déterminer qui est le propriétaire de l'argent, lequel doit subir la perte. Cette approche n'est pas très orthodoxe comparée aux cas similaires de fraudes informatiques,

(...suite)

- vi. le coût de procédures de rechange;
- vii. les procédures généralement utilisées pour des types semblables d'entreprises et d'applications de paiement; et
- viii. la question de savoir s'il y a déjà une relation d'affaires entre les parties.

Et par l'article 5(2) de cette même règle :

- i. la demande de plusieurs formes de renseignements sur l'identité, et la confirmation de ces renseignements dans les bases de données des clients;
- ii. l'obtention de renseignements des bases de données de bureaux de crédit ou de tiers, suivie de la demande au payeur de répondre à certaines questions tirées de ces bases de données;
- iii. l'envoi au payeur d'un élément d'information particulier à une adresse vérifiée de façon indépendante, soit en direct soit en différé, suivi d'une demande au payeur de confirmer ce renseignement;
- iv. l'utilisation de l'identification du demandeur (au téléphone); et
- v. l'utilisation de méthodes biométriques comme la reconnaissance de la voix.

143. Selon les faits exposés dans le jugement, la démarche nécessaire à cette fin consiste à obtenir l'ordre de virement (par télécopieur), un formulaire signé, une vérification de la signature, une vérification téléphonique au moyen de questions à caractère personnel et une contre-vérification par un supérieur : *M'Boutchou c. Banque de Montréal*, 2008 QCCS 5561, par. 59-77.

144. 2019 QCCA 1678.

où les tribunaux analysent habituellement la responsabilité des parties¹⁴⁵. En invoquant l'arrêt *Compagnie d'assurances générales Co-Operators c. Coop fédérée*¹⁴⁶, un notaire fraudé par un tiers (pirate informatique) pourrait-il prétendre que l'argent détenu dans un compte en fidéicommiss ne lui appartient pas, et qu'il ne peut être tenu responsable ?

Il faut distinguer, d'une part, entre les affaires *M'Boutchou c. Banque de Montréal*¹⁴⁷ et *Compagnie d'assurances générales Co-Operators c. Coop fédérée*¹⁴⁸, dont les donneurs d'ordre étaient une simple entreprise (respectivement une PME et une grande coopérative), et, d'autre part, le notaire astreint à un environnement juridique plus rigoureux.

En effet, le notaire est assujéti à des règles déontologiques et à une obligation de vérification de l'identité du client de même qu'à une vérification de la régularité de l'ordre de paiement¹⁴⁹. Il est possible de s'interroger au sujet de la vision de la Cour d'appel dans l'éventualité où le demandeur aurait été un notaire et non la Coop fédérée. L'article 43, al. 1 de la *Loi sur le notariat* indique que « [l]e notaire doit, par tout moyen raisonnable, vérifier l'identité, la qualité et la capacité des parties à un acte notarié dont il reçoit la signature »¹⁵⁰. Cette disposition est complétée par l'article 18 du *Règlement sur la comptabilité en fidéicommiss des notaires* suivant lequel le notaire « doit vérifier, conformément au règlement pris en application de l'article 91 du Code des professions (chapitre C-26), l'identité d'une personne qui lui remet une somme ou un bien pour le bénéfice d'un client »¹⁵¹. Cette disposition est lue conjointement avec l'article 6 du *Règlement sur la tenue des dossiers et des études des notaires*¹⁵², lequel prévoit que « l'identité se fait au moyen de deux documents de source fiable et indépendante », dont l'un d'entre eux comporte une photographie¹⁵³. Cette disposition rap-

145. *M'Boutchou c. Banque de Montréal*, 2008 QCCS 5561.

146. 2019 QCCA 1678.

147. 2008 QCCS 5561.

148. 2019 QCCA 1678.

149. *Règlement sur la comptabilité en fidéicommiss des notaires*, RLRQ, c. N-3, r. 5.2, art. 18-27.

150. RLRQ, c. N-3.

151. *Règlement sur la comptabilité en fidéicommiss des notaires*, RLRQ, c. N-3, r. 5.2.

152. RLRQ, c. N-3, r. 17.

153. L'article 6, al. 2, de ce règlement prévoit notamment, les documents suivants : « 1^o dans le cas d'une personne physique : a) un permis de conduire; b) un acte de naissance; c) une carte d'assurance maladie; d) un passeport; 2^o dans le cas (à suivre...)

pelle le *Règlement sur l'accès aux services bancaires de base*¹⁵⁴ adopté en vertu de la *Loi sur les banques*¹⁵⁵. Dans le domaine bancaire, cette disposition n'empêche pas les fraudeurs d'ouvrir de faux comptes de banque, et il en va de même pour les clients des notaires. L'important est de savoir à quel standard est tenu le notaire dans cette vérification, compte tenu des moyens technologiques mis à sa disposition.

Dans la décision *M'Boutchou c. Banque de Montréal*¹⁵⁶, le juge Lalonde souligne que les « banques doivent démontrer une adaptation qui reflète les attentes des clients », lesquels utilisent régulièrement les moyens technologiques¹⁵⁷. Il ajoute que « [d]eux méthodes semblent se démarquer avec comme objectif de sécuriser le processus d'identification et de transmission des données par la technologie internet », soit « l'identification biométrique (qui se rapporte aux caractéristiques d'une personne) et la cryptographie à clé publique (technique qui assure la sécurité durant la transmission de l'information) »¹⁵⁸, tout en concluant comme suit :

[C]e serait placer la barre trop haute [sic] que d'exiger, en l'instance, que BMO ait été munie de cette technologie en 2005. Mais à l'aube d'une économie instable, d'une période de resserrement du crédit et de difficultés financières, ne serait-il pas approprié que le plus haut niveau de sécurité protège les transactions électroniques faites par les clients des institutions financières ?¹⁵⁹

Quinze ans après les faits de cette histoire, comment se manifeste l'attente raisonnable du client ? La biométrie s'est raffinée et elle est maintenant utilisée à grande échelle, notamment par l'identification pour l'utilisation d'un téléphone intelligent (iPhone,

(...suite)

d'un organisme visé au paragraphe 2 du premier alinéa de l'article 4, un document émis par un organisme public prouvant son existence et indiquant son nom et son adresse ainsi que le nom de ses administrateurs, tel : a) un certificat de constitution ou d'immatriculation; b) une copie du rapport annuel le plus récent; c) une copie des statuts de constitution ou des statuts constitutifs et des statuts de fusion; d) une copie des lettres patentes; e) un contrat de société ou un contrat d'association ».

154. DORS/2003-184, art. 4 et annexe.

155. L.C. 1991, ch. 46, art. 448.1(3), 458.1(2) et 459.4.

156. 2008 QCCS 5561.

157. *M'Boutchou c. Banque de Montréal*, 2008 QCCS 5561, par. 48.

158. *M'Boutchou c. Banque de Montréal*, 2008 QCCS 5561, par. 50.

159. *M'Boutchou c. Banque de Montréal*, 2008 QCCS 5561, par. 51.

Samsung, etc.)¹⁶⁰. La cryptographie¹⁶¹, procédé particulièrement bien rodé, est à la base de la technologie du registre distribué (incluant la chaîne de blocs)¹⁶². Ces technologies participent au contrat intelligent (*smart contract*)¹⁶³ et à l'intelligence artificielle¹⁶⁴. Ajoutons la réflexion au sujet d'une identité numérique¹⁶⁵. Contrairement à la croyance populaire, nourrie par diverses révélations concernant des vols de données dans des institutions financières¹⁶⁶, celles-ci investissent des ressources importantes, en termes de personnel et d'argent, pour assurer une meilleure sécurité et répondre aux attentes raisonnables de leurs clients.

Parmi ces innovations, les institutions financières collaborent avec la société de télécommunications TELUS dans le cadre du projet Assyst Paiement, comme nous l'avons souligné plus haut¹⁶⁷. Cet outil répond aux risques liés aux délai de paiement et à l'identification.

Or, si le droit bancaire enseigne que les banques doivent redoubler de prudence, il ne faut pas oublier que le client, ici le notaire, ne doit pas non plus baisser la garde. Que ce soit Assyst Paiement, la technologie du registre distribué ou tout autre outil technologique performant, le talon d'Achille du notaire concerne l'identification

160. FINEXTRA, « RBC rolls out digital ID verification for account opening », 16 mars 2020, en ligne : <https://www.finextra.com/newsarticle/35457/rbc-rolls-out-digital-id-verification-for-account-opening?utm_medium=news-flash&utm_source=2020-3-16&member=120460>. Voir également : Robee KRISHAN et Reza MOSTAFAVI, « Biometric Technology: Security and Privacy Concerns », (2018) 22(1) *Journal of Internet Law* 19.

161. Nathan K. MCGREGOR, « The Weak Protection of Strong Encryption: Passwords, Privacy, and Fifth Amendment Privilege », (2010) 12(3) *Vand. J. Ent. L. & Prac.* 581; A. Michael FROOMKIN, « The Metaphor is the Key: Cryptography, the Clipper Chip, and the Constitution », (1995) 143(3) *U. Pa. L. Rev.* 709.

162. Thibault SCHREPEL, « Collision by Blockchain and Smart Contracts », (2019) 33(1) *Harv. J.L. & Tech.* 117.

163. Reza MORADINEJAD, « Le Contrat intelligent, nouveau vecteur de confiance dans les relations contractuelles : réalité ou rêve », (2019) 60(3) *C. de D.* 623.

164. Jocelyn MACLURE ET MARIE-NOËLLE SAINT-PIERRE, « Le nouvel âge de l'intelligence artificielle : une synthèse des enjeux éthiques », (2018) 30(3) *C.P.I.* 741; Pierre-Luc DÉZIEL, « Les limites du droit à la vie privée à l'ère de l'intelligence artificielle : groupes algorithmiques, contrôle individuel et cycle de traitement de l'information », (2018) 30(3) *C.P.I.* 827.

165. Alexandre DUVAL, « Une identité numérique pour les Québécois d'ici 2021 », *Radio-Canada*, 11 décembre 2019.

166. Voir *supra*, notes 123-128 et le texte correspondant.

167. Voir *supra*, section 1.1.2.2.

et l'authentification du client. Simplement exprimé par quelques dispositions réglementaires, cette obligation d'identification est de plus en plus lourde à assumer compte tenu de l'imagination des fraudeurs¹⁶⁸. À titre d'illustration, les cas d'hameçonnage se sont grandement perfectionnés comme le démontre la décision *Compagnie d'assurances générales Co-Operators c. Coop fédérée*¹⁶⁹. En outre, ces problèmes d'identification soulèvent également le danger d'instrumentaliser le notaire afin d'obtenir sa collaboration, involontaire, dans une fraude liée au blanchiment d'argent.

En conséquence, il serait pertinent de réfléchir sérieusement à adapter l'article 18 du *Règlement sur la comptabilité en fidéicommiss des notaires*¹⁷⁰ et l'article 6 du *Règlement sur la tenue des dossiers et des études des notaires*¹⁷¹ aux pratiques commerciales et technologiques du XXI^e siècle. Obligation devrait également être faite aux notaires d'utiliser le système Assyst Paiement, à tout le moins dans certaines circonstances.

2.2 Compte en fidéicommiss

Le compte en fidéicommiss se singularise par le fait que le titulaire détient l'argent appartenant à autrui, contrairement au compte courant ou au compte commercial. Dans plusieurs circonstances, les commerçants¹⁷² et les professionnels peuvent ou doivent détenir un tel compte. Dans ce dernier cas, les ordres professionnels¹⁷³,

168. Outre les méthodes déjà énoncées, notons les cas de négligence grossière : *Banque Laurentienne du Canada c. Abdul-Wahab*, 2001 CanLII 151 (QC C.S.).

169. 2019 QCCA 1678. Voir également, au sujet des notaires : Philippe ORFALI, « Ils volent des millions aux notaires », *Journal de Montréal*, 14 janvier 2019, en ligne : <<https://www.tvanouvelles.ca/2019/01/14/ils-volent-des-millions-aux-notaires-1>>.

170. RLRQ, c. N-3, r. 5.2.

171. RLRQ, c. N-3, r. 17.

172. Il s'agit d'un compte que doivent détenir les commerçants ou les entreprises en vertu de certaines lois particulières. Le cas type concerne l'obligation pour le commerçant de déposer dans un compte en fidéicommiss soit les sommes reçues avant l'exécution du contrat, soit celles qui ont été reçues après la conclusion du contrat, dans le cas où celui-ci fait l'objet d'un droit de résolution, obligeant ainsi de conserver les sommes jusqu'à la fin de cette période, soit lorsque le contrat doit être exécuté plus de deux mois après sa conclusion : *Loi sur la protection du consommateur*, RLRQ, c. P-40.1, art. 254-256.

173. *Code des professions*, RLRQ, c. C-26, art. 89.

comme la Chambre des notaires¹⁷⁴ ou le Barreau du Québec¹⁷⁵, autorisent leurs membres à détenir un compte en fidéicommiss aux fins de leurs activités professionnelles. Contrairement aux lois de protection du consommateur, qui ne prévoient que des dispositions de nature générale relativement au compte en fidéicommiss, cet encadrement est de loin beaucoup plus explicite.

Le *Règlement sur la comptabilité en fidéicommiss des notaires* prévoit explicitement le protocole à suivre pour la gestion d'un chèque dans le compte en fidéicommiss¹⁷⁶. D'abord, en ce qui concerne le dépôt d'un chèque, l'article 21 indique que le chèque doit être déposé par un notaire dans son compte en fidéicommiss à la condition qu'il soit « libellé à son ordre, à celui de la société titulaire du compte ou à l'ordre d'un client. Dans ce dernier cas, il ne peut l'être que s'il comporte l'endossement du client et une mention qu'il est fait pour dépôt seulement dans ce compte ». Ensuite, le débours du compte peut être effectué par un chèque tiré au nom du notaire en fidéicommiss, numéroté consécutivement¹⁷⁷. Si ce point ne soulève aucun problème particulier, l'article 27, al. 1(1^o) impose au notaire, avant la clôture d'un acte, l'obligation de « vérifier que les sommes ou les biens que son client lui a remis à cette fin sont suffisants pour permettre l'exécution du dossier et que les ordres de paiement ont été compensés afin de s'assurer de leur disponibilité »¹⁷⁸ et de contrôler rigoureusement les sommes déposées dans son compte en fidéicommiss, notamment en exerçant « un suivi sur les chèques et autres ordres de paiement dans les 6 mois de leur émission afin de s'assurer de leur encaissement »¹⁷⁹.

L'obligation imposée au notaire par l'article 27, al. 1 doit être lue conjointement avec les principes généraux de droit bancaire. La jurisprudence n'oblige aucunement le client d'une banque, qu'il soit

174. *Règlement sur la comptabilité en fidéicommiss des notaires*, RLRQ, c. N-3, r. 5.2, art. 1.

175. *Règlement sur la comptabilité et les normes d'exercice professionnel des avocats*, RLRQ, c. B-1, r. 5, art. 35.

176. *Règlement sur la comptabilité en fidéicommiss des notaires*, RLRQ, c. N-3, r. 5.2, art. 21, 25, 27.

177. *Règlement sur la comptabilité en fidéicommiss des notaires*, RLRQ, c. N-3, r. 5.2, art. 25.

178. *Règlement sur la comptabilité en fidéicommiss des notaires*, RLRQ, c. N-3, r. 5.2, art. 27, al. 1(1^o).

179. *Règlement sur la comptabilité en fidéicommiss des notaires*, RLRQ, c. N-3, r. 5.2, art. 27, al. 1(4^o).

commercial (averti ou non), ou un consommateur, à vérifier ses états bancaires, à moins que cette obligation ne soit stipulée dans un contrat bancaire¹⁸⁰. Ce type de clause, appelée accord de vérification de compte, est une clause exonératoire qui existe depuis une centaine d'années. Elles ont été validées par les tribunaux, lorsqu'elles sont claires et non ambiguës. En cas de doute, elles s'interprètent en faveur du client¹⁸¹. De nos jours, ces clauses sont devenues des clauses de style systématiquement insérées dans les contrats bancaires. Ainsi, l'obligation du notaire de vérifier ses états bancaires, et surtout les chèques, découle à la fois de l'article 27, al. 1 du *Règlement sur la comptabilité en fidéicomis des notaires*¹⁸² et des principes de droit bancaire.

Bien que le compte en fidéicomis soit strictement contrôlé par les syndicats d'ordres professionnels, il faut reconnaître qu'il est attrayant aux yeux des fraudeurs. Le problème fondamental est de déterminer les obligations et la responsabilité des intervenants en cas de fraude dans le compte en fidéicomis, notamment lors d'un dépôt frauduleux. Aux fins de la discussion, tenons pour acquis que la fraude émane d'un tiers (employé ou autre) et non du notaire.

Comment se produit la fraude ? Il existe plusieurs cas de figure.

Premièrement, il peut s'agir du dépôt frauduleux d'un effet de commerce. Si le notaire n'est pas impliqué directement, l'un de ses employés peut l'être. Les règles concernant le dépôt frauduleux que nous avons exposées ci-dessus demeurent pertinentes, c'est-à-dire que la banque d'encaissement doit vérifier l'endossement du détenteur du chèque ou de la traite bancaire, lors du dépôt¹⁸³.

Deuxièmement, outre le cas d'un dépôt frauduleux se produisant une seule fois, il peut survenir une série de transactions inhabituelles dans le compte en fidéicomis. Le cas échéant, il s'agira habituellement d'un employé malintentionné, souvent motivé par la cupidité ou par le besoin immédiat d'argent pour couvrir des problèmes de drogues ou de jeu, par exemple. En pratique, devinant

180. Voir *supra*, notes 105-106 et le texte correspondant.

181. Voir *supra*, notes 105-106 et le texte correspondant.

182. RLRQ, c. N-3, r. 5.2.

183. Voir *supra*, section 2.1.1.1.2.

que le stratagème fonctionne, le fraudeur recommencera. Au fil du temps, après un contrôle serré des finances de la société, il sera démasqué. Cette question dépasse le cadre strictement notarial pour viser tous les employeurs. Dans une telle fraude, il est parfois difficile de déterminer qui du notaire (employeur) ou de la banque doit assumer la perte. Dans le célèbre arrêt *Boma* concernant une fraude de chèque, le juge La Forest, dissident, avait soulevé la réflexion suivante :

En ce qui concerne l'employeur-tireur et la banque-accepteur, il faut se demander qui doit assumer le risque de perte et qui est le mieux placé pour réduire au minimum ce risque. À ces deux questions, il faut, selon moi, répondre : l'employeur-tireur. Dans un cas comme celui qui nous occupe, la banque-accepteur reçoit habituellement les chèques frauduleux de l'un de ses clients qui se fait passer pour l'endossataire ou le détenteur du chèque. Puisque le preneur nommé est généralement un étranger pour la banque, l'exigence d'endossement du chèque s'avère le plus souvent un moyen inefficace de la protéger contre la fraude. Comme le montrent les faits de la présente affaire, le fraudeur peut assez aisément falsifier l'endossement du preneur nommé et la banque n'a aucun moyen de vérifier l'authenticité de la signature. En revanche, l'employeur-tireur est beaucoup mieux placé pour mettre fin à ce genre de fraude et est au moins aussi bien placé pour assumer toute perte subie. Il va sans dire que tout risque de perte auquel est exposée une grande entreprise est généralement couvert par une assurance contre les détournements. Il est également possible de déceler la fraude sur grande échelle par des vérifications et d'autres mesures de protection. Si le tireur est une petite entreprise, comme c'est le cas en l'espèce, il est alors très bien placé pour déceler rapidement la fraude et pour réduire ainsi au minimum la perte.¹⁸⁴

Indépendamment de la question de l'assurance détenue par un employeur, il faut reconnaître que ce point de vue est suffisamment convaincant pour que les banques exigent que leurs clients prennent des mesures pour diminuer les risques de fraude, étant par ailleurs entendu que ce risque ne peut être totalement écarté. Se référant à ce point de vue du juge La Forest dans l'arrêt *Boma*, les juges Côté et Rowe considèrent plus récemment que cette approche « est à la fois juste et efficace » pour imputer la perte à la personne qui est la mieux placée pour la prévenir, notamment en adoptant des politiques à cet égard¹⁸⁵.

184. *Boma Manufacturing Ltd. c. Banque Canadienne Impériale de Commerce*, [1996] 3 R.C.S. 727, par. 95.

185. *Teva Canada Ltée c. TD Canada Trust*, 2017 CSC 51, par. 129-131. À l'instar du juge La Forest dans l'arrêt *Boma Manufacturing Ltd. c. Banque Canadienne* (à suivre...)

Les situations de fraudes multiples dans un compte en fiducie ou en fidéicommiss trouvent occasionnellement écho en jurisprudence. L'arrêt *124329 Canada inc. c. Banque Nationale du Canada/National Bank Of Canada* illustre bien ce cas de figure¹⁸⁶. En l'espèce, les frères Jackson, quatre hommes d'affaires aguerris, désiraient investir une somme de 500 000 \$ dans la relance d'une entreprise et ont été floués dans cette aventure par un certain M^e Blanchet, avocat (radié par la suite), et par messieurs Farr et Muro. Sous un angle technique, la transaction financière s'est matérialisée ainsi. Dans un premier temps, l'avocat a tiré un chèque de son compte en fidéicommiss, payable à une entreprise dont il avait déjà été membre auparavant. Le chèque portait un endossement restreint : « pour dépôt seulement au crédit de M^e Martin Blanchet ». Dans les faits, l'endossement a été forgé par M^e Blanchet et celui-ci n'avait pas l'intention que le bénéficiaire obtienne l'argent. Dans un deuxième temps, le chèque a été déposé par M^e Blanchet dans son compte courant. À ce moment, le chèque portant un double endossement, la banque a « garanti l'endossement et honoré la transaction »¹⁸⁷. Dans un troisième temps, et au cours de la même journée que les transactions précédentes, M^e Blanchet a ordonné que les fonds soient virés dans son autre compte en devises américaines. Dans un quatrième temps, M^e Blanchet a tiré une traite bancaire près de deux mois plus tard au montant de 500 000 \$ US et payable au nom d'une tierce compagnie. Comme le rappelle le juge Kasirer de la Cour d'appel, l'argent étant un bien fongible, le suivi de cet argent par les Jackson était pratiquement impossible¹⁸⁸.

Bien que ce cas concerne un avocat, il pourrait s'appliquer à un employé d'un notaire. Outre la responsabilité pour son employé, comme le soulignait le juge La Forest, notons que lorsque la fraude émane du titulaire du compte, les tribunaux québécois ont tenté d'imputer à la banque une responsabilité fondée sur la connaissance que celle-ci avait, ou aurait dû avoir, de la fraude.

(...suite)

Impériale de Commerce, [1996] 3 R.C.S. 727, les juges Côté et Rowe étaient également dissidents. Voir également : *Gescoro inc. c. Rémillard*, 2019 QCCA 973 (conf. par C.S.C., n^o 38790, 6 février 2020).

186. 2011 QCCA 226.

187. *124329 Canada inc. c. Banque Nationale du Canada/National Bank Of Canada*, 2011 QCCA 226, par. 17 et 19.

188. *124329 Canada inc. c. Banque Nationale du Canada/National Bank Of Canada*, 2011 QCCA 226, par. 28.

Dans l'arrêt *124329 Canada inc.*, la Cour d'appel déclare que la banque est responsable de n'avoir pas agi en personne raisonnable et de n'avoir pas respecté son obligation de diligence (*duty of care*) dans les circonstances. La conduite de l'avocat fraudeur aurait dû alerter la banque : le retrait d'une somme substantielle de son compte en fidéicommiss, le nombre important de transactions qui se sont produites au même moment (rendant difficile la traçabilité des fonds), le transfert d'une part importante des fonds détenus en fidéicommiss vers le compte courant, le chèque payable à une tierce partie inconnue de la banque et deux chèques d'un montant substantiel portaient un double endossement¹⁸⁹. Le juge Kasirer suggère qu'il convient de rechercher des « strong signs of misdealing before deciding a bank can be held liable for not having taken measures to prevent it »¹⁹⁰. Cette vision s'inscrit dans le sillon du juge La Forest, qui a déclaré dans l'arrêt *Citadelle (La), Compagnie d'assurances générales c. Banque Lloyds du Canada* que, parfois :

une banque sera tenue, du fait qu'elle connaît les affaires de son client, de s'informer de la possibilité qu'il y ait détournement de fonds en fiducie. [...] Si la banque omet de demander les renseignements appropriés, elle aura une connaissance présumée du manquement à une obligation fiduciaire. Dans ces circonstances, il y a enrichissement sans cause de la banque et elle doit donc rendre l'avantage qu'elle a obtenu aux dépens du demandeur.¹⁹¹

Concrètement, le fraudeur est le premier responsable, mais devant son insolvabilité, les victimes ont intenté un recours contre la banque.

Troisièmement, la fraude peut provenir d'un pirate informatique (*hacker*). Le cas échéant, elle peut prendre plusieurs aspects. L'idée est d'usurper l'identité du notaire pour s'infiltrer dans son ordinateur afin de soulager ce dernier de ses fonds en y effectuant des transferts électroniques de fonds frauduleux¹⁹². Hélas, malgré

189. *124329 Canada inc. c. Banque Nationale du Canada/National Bank Of Canada*, 2011 QCCA 226, par. 69.

190. *124329 Canada inc. c. Banque Nationale du Canada/National Bank Of Canada*, 2011 QCCA 226, par. 67.

191. [1997] 3 R.C.S. 805, par. 52. L'article 206(1) de la *Loi sur les banques*, L.R.C. (1985), ch. B-1, dont il est question dans cette décision, est substantiellement repris dans son esprit, bien que la phraséologie ait été modifiée, par l'article 437(3) de l'actuelle *Loi sur les banques*, L.C. 1991, ch. 46.

192. Voir *supra*, section 2.1.2.2.

les précautions quant à la signature numérique du notaire et à la gestion des codes secrets¹⁹³, la réalité dépasse la fiction, s'agissant d'une situation qui doit être sérieusement considérée¹⁹⁴.

CONCLUSION

À l'aune de ces développements, une conclusion s'impose. En matière de sécurité des transactions, la traite bancaire, et surtout le chèque, représentent des instruments de paiement archaïques et inadéquats pour assurer la sécurité d'une transaction, en particulier en présence d'un notaire. Les paiements électroniques sont compensés et réglés plus rapidement, et ils n'offrent habituellement aucune possibilité de contrordre. Malgré les développements technologiques qu'il a favorisés au cours des dernières années pour faciliter la compensation du chèque, il est clair que Paiements Canada encourage la migration des transferts de fonds vers les paiements électroniques. Au demeurant, le système Assyst Paiement est particulièrement adapté pour la pratique notariale et permet d'éviter des cas de fraudes reliés aux effets papier et aux délais de compensation.

193. NOTARIUS (CHAMBRE DES NOTAIRES DU QUÉBEC), *CertifIO pour Professionnels*, 2020, en ligne : <<https://notarius.com/certifio/professionnels/cnq/>>.

194. Philippe ORFALI, « Ils volent des millions aux notaires », *Journal de Montréal*, 14 janvier 2019, en ligne : <<https://www.tvanouvelles.ca/2019/01/14/ils-volent-des-millions-aux-notaires-1>>; CHAMBRE DES NOTAIRES DU QUÉBEC, « Notaires visés par des fraudeurs : aucun client lésé », communiqué de presse, 14 janvier 2019, en ligne : <<https://www.cnq.org/fr/89-0-salle-de-presse-notaires-vises-par-des-fraudeurs-aucun-client-lese.html>>; Simon-Pierre LORANGE, « Vols d'identité : faute de coupable, qui doit payer ? », *La Presse*, 26 juin 2019, section Actualités.