”La maîtrise des risques juridiques en cas de paiements frauduleux”

Anthony Maymont

La maîtrise des risques juridiques en cas de paiements frauduleux

Anthony MAYMONT
Maître de conférences HDR en droit privé
Membre du Centre de recherche Michel de l'Hospital (UPR 4232)
Université Clermont Auvergne

Résumé : La fraude aux moyens de paiement, et en particulier celle des paiements à distance, se développe et se transforme. La maîtrise des risques juridiques est alors indispensable afin d'assurer la sécurité des opérations, tant pour les clients que pour les banquiers. Elle a même été renforcée sous l'impulsion du législateur et du juge. Or, s'il exige une vigilance constante des parties, ce renforcement demeure ambivalent car le risque final ne sera généralement supporté que par l'une d'elles.

1. L'exposition des parties aux paiements frauduleux. – Les fraudes et escroqueries ne cessent de se développer[1]. Celles-ci prennent diverses formes telles que des escroqueries aux livrets et aux crédits[2], des arnaques au *trading* (Forex) et aux crypto-actifs[3], ainsi que de fausses offres d'investissement[4]. Le paiement, quant à lui, n'est pas non plus épargné. Il fait face à des évolutions significatives liées aux innovations technologiques, lesquelles peuvent être sources de nouveaux types de fraudes. Le constat est celui d'un développement manifeste des moyens de paiements scripturaux dans la mesure où les paiements par carte et ceux par virement représentaient respectivement 56,9 % et 17,1 % du volume des transactions en 2021[5]. Au regard de la place centrale de ces opérations de paiement dans le secteur économique, le législateur est intervenu afin de sécuriser leur exécution. L'intérêt est de réduire la fraude tout en préservant la confiance des clients lors de l'utilisation des services de paiement à distance en ligne.

Les clients comme les banquiers sont exposés à divers risques en la matière. Pour les clients, ce risque se traduit essentiellement par une perte financière résultant d'un piratage, d'un hameçonnage ou *phishing*, voire d'une négligence grave relative à la préservation de la sécurité de leurs données de sécurité personnalisées. Pour le banquier, ce risque peut prendre d'autres formes, lesquelles se cumulent souvent avec celui d'une perte financière. Il s'agit du risque réputationnel, lequel n'est pas à négliger, et du risque juridique[6]. En matière de services de paiement, la survenance de paiements frauduleux constitue un risque notable.

2. L'évolution de la fraude aux paiements. – La fraude aux moyens de paiement tend à croître en fonction du rythme de progression des flux de paiement. À la suite de trois années de progression, le constat a toutefois été celui d'un recul des fraudes en 2021 même si celles-ci restent présentes. Les paiements à distance représentent 70 % de la fraude alors qu'ils ne constituent que 20 % des transactions nationales. Néanmoins, en comparaison aux années précédentes, le taux de fraude des paiements par internet a significativement baissé en raison

[1] V. Task Force nationale de lutte contre les arnaques, *Guide de prévention contre les arnaques,* 2022.
[2] V. not. J. Lasserre Capdeville, « Les *« arnaques aux crédits »* », *RD bancaire et fin.* juill.-août 2022, alerte n° 85.
[3] V. *Dossier L'encadrement des crypto-actifs,* dir. N. Kilgus, Hors-série, *Banque et droit* janv. 2022.
[4] ACPR-AMF, Pôle commun Assurance Banque Épargne, *Rapport d'activité 2021,* juin 2022, p. 11.
[5] OSMP, *Rapport annuel 2021*, Banque de France, juill. 2022, p. 10.
[6] Arr. 3 nov. 2014 relatif au contrôle interne des entreprises du secteur de la banque, des services de paiement et des services d'investissement soumises au contrôle de l'Autorité de contrôle prudentiel et de résolution, art. 10, k).

de la mise en place de l'authentification forte[7]. Sur ce point, la directive sur les services de paiement du 25 novembre 2015, dite « DSP 2 », a eu un rôle majeur[8].

Cette directive a été transposée par l'ordonnance n° 2017-1252 du 9 août 2017 dont les dispositions sont entrées en vigueur le 13 janvier 2018[9]. Ce texte vise la gestion des risques cyber, et en particulier renforce la protection des utilisateurs de services de paiement. À cet effet, il institue l'authentification forte pour les clients tout en modifiant les procédures de contestation des paiements. Partant, cela participe de la prévention des risques juridiques qui est le fondement de la maîtrise de ceux-ci.

3. L'objectif de prévention des risques juridiques. – Comme évoqué, les paiements à distance sont très majoritairement concernés par la fraude. Ils feront alors l'objet de la présente étude, à l'exclusion des paiements par chèque pour lesquels la distinction entre le chèque faux et celui falsifié est ancrée depuis longtemps[10]. Au cas particulier, les difficultés surviennent lorsque le client déclare ne pas être à l'origine du paiement. Le cas échéant, se considérant victime d'une fraude ou ayant simplement fait preuve d'une négligence, il contestera les opérations qu'il estime ne pas avoir autorisées. Une telle contestation, laquelle sera généralement à l'origine d'un contentieux, doit être distinguée de l'opposition au paiement. Alors que la contestation concerne les opérations ayant déjà été exécutées, l'opposition interdit l'exécution d'ordres n'ayant pas encore été émis[11].

L'objectif premier de la réglementation est donc la protection des utilisateurs de services de paiement à l'égard des risques liés aux paiements électroniques. Cela ressort clairement de la DSP 2, laquelle souligne que la sûreté et la sécurité des services de paiement sont vitales pour le bon fonctionnement du marché desdits services[12]. *A fortiori,* et outre l'utilisateur, la caution de celui-ci peut également engager la responsabilité civile contractuelle de droit commun de la banque en présence d'opérations de paiement non autorisées[13]. La maîtrise des risques juridiques est ainsi indispensable afin d'assurer la sécurité des paiements, tant pour les utilisateurs que pour le banquier dont la responsabilité n'est plus forcément engagée sur une faute mais sur la survenance du risque. Aussi, les évolutions de la réglementation assurent-elles un renforcement de la maîtrise des risques juridiques en la matière ? Une réponse nuancée s'impose. En effet, si l'apparence d'un renforcement de la maîtrise des risques juridiques est indéniable (I), celui-ci reste cependant ambivalent selon que le payeur ou le banquier est concerné (II).

---

[7] OSMP, *op. cit.,* p. 16.
[8] Dir. (UE) 2015/2366 du Parlement européen et du Conseil du 25 nov. 2015 concernant les services de paiement dans le marché intérieur, *JOUE* L 337/35 du 23 déc. 2015.
[9] Ord. n° 2017-1252 du 9 août 2017 portant transposition de la directive 2015/2366 du Parlement européen et du Conseil du 25 nov. 2015 concernant les services de paiement dans le marché intérieur.
[10] C. Kleiner, « La responsabilité civile du banquier tiré en matière de chèque », *in La responsabilité civile du banquier aujourd'hui,* dir. J. Lasserre Capdeville, préf. Th. Bonneau, LexisNexis, 2022, p. 169 *sq.*, spéc. n° 362 *sq.*
[11] N. Kilgus, « L'évolution des procédures de contestation des paiements », *RD bancaire et fin.* mars-avr. 2018, dossier n° 11.
[12] Dir. (UE) 2015/2366, considérant n° 7.
[13] Cass. com., 9 févr. 2022, n° 17-19441, *Bull. civ.* IV ; *Banque et droit* mars-avr. 2022, n° 202, p. 29-30, obs. N. Rontchevsky ; *RCA* mai 2022, comm. n° 133, obs. L. Bloch.

I – Un renforcement apparent de la maîtrise des risques juridiques

4. La maîtrise des risques juridiques fait l'objet d'un renforcement apparent émanant de la loi et de la jurisprudence. Elle s'exprime tant par l'instauration d'une exigence d'authentification forte (A) que par l'effectivité des obligations professionnelles du banquier (B). Cela contribue à la sécurité des paiements à la fois pour l'utilisateur des services de paiement et le prestataire, à savoir généralement le banquier.

A – L'instauration d'une exigence d'authentification forte

5. Le passage du protocole *3D Secure* à l'authentification forte. – Les établissements de crédit ont longtemps utilisé le protocole *3D Secure* (version 1), lequel a été instauré en 2008 afin d'améliorer la sécurité des transactions. En l'occurrence, l'authentification du porteur s'effectue à travers trois éléments. Le premier concerne le numéro présent sur la carte bancaire. Le deuxième est relatif au cryptogramme mentionné au verso de cette dernière. Le troisième vise le code unique transmis par SMS – *One Time Password* [OTP] – sur le téléphone portable du client[14]. Or, face aux faiblesses assortissant ce protocole afin de juguler la fraude, les protocoles d'authentification ont dû évoluer. Ce faisant, la DSP 2 a institué une authentification forte dont l'entrée en vigueur était prévue au 14 septembre 2019. Toutefois, en raison des difficultés liées à sa mise en place tant par les professionnels que les usagers, l'application effective de ce dispositif a finalement été reportée au 15 mai 2021[15].

L'authentification forte est prévue à l'article L. 133-44 du Code monétaire et financier, lequel impose aux prestataires de services de paiement de la mettre en œuvre. Sa définition, quant à elle, se situe à l'article L. 133-4, f) du même Code. Celui-ci dispose que l'authentification forte constitue « *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* ». À la lecture de ces éléments, il importe de mesurer l'application pratique d'un tel dispositif.

6. L'application pratique de l'authentification forte. – Au regard des exigences énoncées par l'article précité, il ressort que le protocole *3D Secure* ne satisfait pas à celles-ci. Cela a notamment été relevé par l'Autorité bancaire européenne, laquelle a considéré que le numéro de carte avec le code de vérification ou cryptogramme – CVV signifiant *Card Verification Value* – et la date d'expiration ne constituaient pas un élément de connaissance. Au contraire, et afin qu'un appareil soit assimilé comme une « *possession* », un moyen fiable permettant de confirmer celle-ci doit exister comme avec la réception d'un élément de validation dynamique sur l'appareil[16]. C'est la raison pour laquelle un renforcement du dispositif existant a été opéré, ce qui aboutit corrélativement à une maîtrise des risques juridiques.

---

[14] J. Huet et M. Espagnon, « Paiement électronique. – Notions juridiques générales », *J.-Cl. Droit bancaire et financier*, Fasc. n° 400, n° 64.

[15] Fédération bancaire française, « 15 mai 2021 : mise en place de l'authentification forte pour tous les achats en ligne », Communiqué de presse, 14 mai 2021 ; V. J. Lasserre Capdeville, « Opérations de paiement à distance : le report de l'authentification forte », *JCP E* 2019, act. n° 666.

[16] *EBA*, *Opinion of the European Banking Authority on the implementation of the RTS on SCA and CSC,* 13 June 2018, EBA-2018-Op-04, § n° 35, p. 7.

Sur un plan pratique, les établissements de crédit recourent à une authentification forte axée sur un boitier qu'ils fournissent eux-mêmes ou via l'utilisation d'un smartphone. Deux situations peuvent en résulter. D'une part, le client devra se connecter à l'application mobile de sa banque en indiquant un mot de passe, ce qui correspond aux facteurs « *connaissance* » et « *possession* ». D'autre part, au lieu du mot de passe, le client peut être amené à entrer une donnée biométrique telle que ses empreintes, ce qui remplit les facteurs « *possession* » et « *inhérence* »[17]. Cette authentification forte, laquelle renforce indéniablement la protection des clients et réduit les risques juridiques pour les parties, est complétée par l'effectivité des obligations professionnelles du banquier.

B – L'effectivité des obligations professionnelles du banquier

7. L'obligation de vigilance *versus* le devoir de non-immixtion du banquier. – La loi et la jurisprudence ne définissent pas spécifiquement l'obligation de vigilance. Du fait de son caractère protéiforme, il n'existerait pas de notion générale de vigilance mais en réalité plusieurs sources légales et jurisprudentielles ayant chacune leur propre régime[18]. Cela étant, la doctrine a apporté une définition, laquelle prévoit que le banquier doit agir en bon professionnel en s'informant – sans contrevenir au devoir de non-immixtion – sur les opérations que ses clients envisagent de réaliser et à avoir suffisamment de discernement pour ne pas intervenir si les circonstances l'imposent[19]. Même si elle peut parfois faire l'objet d'un dévoiement, l'obligation de vigilance en droit bancaire est au cœur de la prévention des risques[20], dont les risques financiers concernés par la présente étude. Elle ne doit pas être confondue avec celle existante en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme qui reste distincte[21]. Partant, il ressort que l'obligation de vigilance s'applique tout au long de l'activité exercée par le banquier. En revanche, elle n'aurait pas à s'appliquer en présence d'un dispositif d'authentification forte, lequel laisse présumer que l'utilisateur des services de paiement est à l'origine de l'opération éventuellement contestée. En de telles circonstances, la responsabilité du banquier ne saurait non plus être recherchée en raison de son devoir de non-immixtion.

La distinction entre l'obligation de vigilance et le devoir de non-immixtion peut sembler ténue. Elle cristallise l'attention des plaideurs, et en particulier des clients, lesquels tentent de démontrer que le banquier aurait dû intervenir pour les alerter voire empêcher les opérations litigieuses. Or, d'une manière générale, le banquier reste tenu à un devoir de non-immixtion, lequel lui interdit toute ingérence dans les affaires de son client[22]. Néanmoins, il se doit de faire preuve de vigilance en présence uniquement d'anomalies tant matérielles qu'intellectuelles,

---

[17] N. Kilgus, « Authentification forte et preuve de la négligence grave de l'utilisateur d'un instrument de paiement », *Mélanges AEDBF France VIII,* dir. B. Bréhier, RB Édition, 2022, p. 43 *sq*., spéc. p. 45.

[18] J. Martinet, « L'obligation de vigilance des banques – Décryptage d'une notion plurielle », *Mélanges AEDBF France VIII,* dir. B. Bréhier, RB Édition, 2022, p. 59 *sq.*, spéc. p. 60.

[19] Th. Bonneau, *Droit bancaire,* 14e éd., LGDJ, 2021, n° 613 ; J. Lasserre Capdeville, M. Storck, M. Mignot, J.-Ph. Kovar et N. Éréséo, *Droit bancaire,* 3e éd., Dalloz, 2021, n° 271.

[20] B. de Belval et A. Maymont, « Le clair-obscur de l'obligation de vigilance du banquier », *Gaz. Pal.* 2 févr. 2021, p. 45 *sq.* ; V. A. Maymont, *La compliance en droit bancaire et financier,* avant-propos N. Kilgus, préf. Th. Bonneau, mare & martin, 2022, n° 55 *sq.*

[21] Cass. com., 21 sept. 2022, n° 21-12335, *Bull. civ.* IV ; *Gaz. Pal.* 8 nov. 2022, p. 37 *sq.*, note M. Roussille ; *JCP E* 2022, 1383, note J. Lasserre Capdeville ; *RD bancaire et fin.* nov.-déc. 2022, comm. n° 156, note Th. Samin et S. Torck ; *Banque* déc. 2022, n° 874, p. 60-61, note P. Storrer.

[22] Cass. com., 27 nov. 2012, n° 11-19311, *D.* 2013, p. 2430-2431, obs. D. R. Martin ; *JCP E* 2013, 1282, n° 20, obs. L. Dumoulin ; Cass. com., 28 juin 2016, n° 14-21256, *JCP E* 2016, 1587, n° 5, obs. Ch. Lassalas.

lesquelles s'apprécient *in concreto*[23]. La nécessité d'une approche au cas par cas explique alors le nombre de contentieux pouvant survenir. Pour autant, il faut constater que l'obligation de vigilance participe indéniablement à la maîtrise des risques juridiques afin d'éviter tout paiement frauduleux. Celle-ci est même assurée par la caractérisation d'un devoir de diligence à la charge du banquier.

8. La caractérisation d'un devoir de diligence du banquier. – Le devoir de diligence du banquier s'exprime à travers la loi sans qu'il ne soit véritablement consacré. Toute la difficulté réside dans son articulation avec le devoir de non-immixtion[24]. Le banquier est effectivement tenu de réaliser correctement les opérations souhaitées par son client. Cependant, la responsabilité du banquier ne pourrait être recherchée si une opération de paiement mal exécutée n'est pas du fait de ce dernier. À titre d'illustration, le banquier est normalement tenu d'exécuter un ordre de virement dès lors que celui-ci est régulier et que le compte bancaire du client fait état d'un solde disponible suffisant[25]. Pour ce faire, il doit s'assurer que l'ordre émane de son client ou de son représentant, faisant que celui-ci doit être pourvu du pouvoir de faire fonctionner les comptes[26].

Le cas échéant, le banquier ne peut donc se soustraire à son obligation de réaliser l'ordre émis par son client. Toutefois, et dans l'hypothèse d'une opération de paiement mal exécutée et sans préjudice de sa responsabilité, le banquier doit uniquement s'efforcer, à la demande de son client, de retrouver la trace de cette opération et lui notifier le résultat de sa recherche sans frais pour ce dernier[27]. Autrement dit, dès que l'ordre est régulier et que le compte bancaire comporte une somme suffisante, la responsabilité du banquier ne peut être engagée. Il doit seulement tenter de récupérer les fonds sans qu'il ne s'agisse d'une obligation de résultat, ce qui marque ainsi les limites de son devoir de diligence. Aussi, et à l'instar de l'obligation de vigilance, le devoir de diligence renforce la maîtrise des risques juridiques. Cela étant, ce renforcement reste ambivalent selon la partie concernée.

II – Un renforcement ambivalent de la maîtrise des risques juridiques

9. Le renforcement de la maîtrise des risques juridiques, s'il est apparent, n'en reste pas moins ambivalent. Il diffère selon la partie concernée, à savoir l'utilisateur des services de paiement ou le payeur et le prestataire de services de paiement ou le banquier. L'un ou l'autre supportera les risques juridiques selon le cas. Une telle distinction se note en présence de l'éventualité d'une faute exclusive du payeur (A) et de la nécessaire preuve des opérations litigieuses par le banquier (B).

---

[23] Th. Bonneau, *op. cit.*, n° 614 ; J. Lasserre Capdeville, M. Storck, M. Mignot, J.-Ph. Kovar et N. Éréséo, *op. cit.*, n° 278.

[24] A. Maymont et J. Lasserre Capdeville, « Le banquier dispensateur de crédit et le devoir de diligence », *RD bancaire et fin.* janv.-févr. 2023, dossier n° 5.

[25] Cass. com., 19 déc. 2000, n° 97-15394, *Bull. civ.* IV, n° 193 ; *RD bancaire et fin.* mars-avr. 2001, comm. n° 46, obs. F.-J. Crédot et Y. Gérard ; *RTD com.* 2001, p. 749-750, note M. Cabrillac.

[26] F. Grua, « Banquier. – Responsabilité en matière de services. – Service de caisse », *J.-Cl. Civil Code,* mars 2021, Fasc. n° 335-30, spéc. n° 50.

[27] C. mon. fin., art. L. 133-22, III.

A – L'éventualité d'une faute exclusive de l'utilisateur de services de paiement

10. L'obligation de préservation de la sécurité du dispositif de sécurité personnalisé. – Aux termes de l'article L. 133-18, alinéa 1 du Code monétaire et financier, le prestataire de services de paiement du payeur est tenu de rembourser immédiatement à ce dernier le montant de l'opération non autorisée à moins qu'il ne soupçonne une fraude de l'utilisateur du service de paiement. Le principe du remboursement immédiat souffre donc d'une exception, laquelle n'est pas sans conséquences. En effet, le banquier aura vocation à diligenter diverses investigations pour confirmer ou non l'existence d'une fraude. Cela peut alors justifier qu'un remboursement immédiat soit difficilement envisageable afin que toutes les recherches soient effectuées. Une telle pratique reste toutefois contestée par les consommateurs. Ce faisant, le législateur a institué des pénalités à l'égard du banquier en cas de non-respect de ses obligations visées par cet article[28].

En tout état de cause, l'utilisateur de services de paiement doit, lorsqu'il reçoit un instrument de paiement, prendre toutes les mesures raisonnables afin de préserver la sécurité de ses données de sécurité personnalisées[29]. Dans le cas contraire, il devra supporter les pertes occasionnées par des opérations de paiement non autorisées lorsque ces pertes résultent d'un agissement frauduleux de sa part ou s'il n'a pas satisfait intentionnellement ou par négligence grave à cette obligation[30]. Dès lors, la responsabilité du banquier ne saurait être engagée lorsque ses clients ont commis des manœuvres frauduleuses ou ont fait preuve d'une négligence grave ayant permis à un fraudeur de réaliser une opération de paiement. En d'autres termes, toute faute exclusive à l'origine du préjudice de l'utilisateur de services de paiement a vocation à mettre hors de cause la banque. Une telle hypothèse est identifiable en pratique, d'autant que les clients victimes d'un préjudice ne mettent pas en cause immédiatement leur banquier. Celui-ci ne sera généralement inquiété que dans un second temps lorsque la récupération des fonds auprès du fraudeur aura été infructueuse, ce qui est souvent le cas.

11. La caractérisation d'une négligence grave de l'utilisateur de services de paiement. – La fraude en matière de paiement à distance survient fréquemment via la technique du *phishing* par laquelle les clients divulguent des informations confidentielles à la suite de la réception d'un courriel. En de telles circonstances, les juges du fond doivent rechercher si les clients n'auraient pas pu avoir conscience du caractère frauduleux du message reçu[31]. Afin de caractériser la négligence grave, ils sont amenés à se référer au comportement d'« *un utilisateur normalement attentif* »[32]. *A fortiori*, la détermination d'une telle négligence est exclusive de toute appréciation de la bonne foi des clients[33]. Ainsi, il suffit que les clients n'aient pas fait preuve d'une vigilance suffisante, laquelle aboutirait à la caractérisation d'une négligence

[28] C. mon. fin., art. L. 133-18 dont l'alinéa 3 a été ajouté par L. n° 2022-1158 du 16 août 2022 portant mesures d'urgence pour la protection du pouvoir d'achat, art. 22.
[29] C. mon. fin., art. L. 133-16, al. 1.
[30] C. mon. fin., art. L. 133-19, IV.
[31] Cass. com., 25 oct. 2017, n° 16-11644, *Bull. civ.* IV ; *JCP E* 2017, 1685, note D. Legeais ; *Banque et droit* janv.-févr. 2018, p. 20-21, obs. Th. Bonneau ; *RD bancaire et fin.* nov.-déc. 2017, comm. n° 233, note Th. Samin et S. Torck ; Cass. com., 24 nov. 2021, n° 20-13767, *JCP E* 2022, 1253, spéc. n° 21, obs. A. Salgueiro.
[32] Cass. com., 28 mars 2018, n° 16-20018, *Bull. civ.* IV ; *RTD com.* 2018, p. 436, obs. D. Legeais ; *Gaz. Pal.* 15 mai 2018, p. 20 *sq.*, obs. J. Lasserre Capdeville ; *JCP E* 2018, 1272, note K. Rodriguez ; *JCP G* 2018, 458, obs. N. Kilgus ; *Contrats conc. consom.* 2018, comm. n° 121, obs. S. Bernheim-Desvaux ; *Comm. com. électr.* 2018, comm. n° 34, obs. G. Loiseau.
[33] Cass. com., 1er juill. 2020, n° 18-21487, *Bull. civ.* IV ; *Banque et droit* nov.-déc. 2020, n° 194, p. 22-23, obs. Th. Bonneau ; *Gaz. Pal.* 20 oct. 2020, p. 59 *sq.*, note M. Roussille ; *JCP E* 2020, 1399, obs. K. Rodriguez.

grave, pour qu'ils soient tenus d'assumer l'entièreté du préjudice subi. Partant, l'absence d'intention ne peut écarter toute faute exclusive de leur part.

En amont de l'intervention du juge, et comme le prévoit l'article L. 316-1 du Code monétaire et financier, tout client personne physique a la possibilité de recourir à un médiateur dans une perspective de résolution amiable des litiges l'opposant à un établissement de crédit. Si l'avis rendu par le médiateur bancaire pourra relever une négligence grave de la part de l'utilisateur du service de paiement, il faut cependant souligner qu'un tel avis est par principe confidentiel[34]. Comme cela est expressément indiqué par le médiateur sur chaque avis rendu, celui-ci ne constitue donc pas une décision, faisant que les parties sont libres de l'accepter ou non[35]. Dans ce dernier cas, il ne pourra pas être produit en justice sauf accord contraire des parties, lesquelles décideraient de lever la confidentialité. Une telle issue pourrait sembler toutefois regrettable dans la mesure où l'intervention du médiateur, tiers indépendant[36], permettrait d'éclairer davantage le juge sur les faits sans que celui-ci ne soit tenu de la solution émise[37]. Si la négligence grave permet au banquier de s'exonérer de toute responsabilité et de prétendre à sa mise hors de cause, encore faut-il qu'il puisse apporter la preuve de la faute de son client. Cela semble particulièrement délicat, surtout si le client n'admet pas une légèreté blâmable de sa part ou avoir été victime d'un *phishing*.

B – La nécessaire preuve des opérations litigieuses par le banquier

12. La négligence grave, une preuve délicate pour le banquier. – Le banquier est confronté, dans la recherche de la preuve de la négligence grave de son client, à une « *probatio diabolica* »[38]. En effet, aux termes de l'article L. 133-23, alinéa 1 du Code monétaire et financier, il incombe au prestataire de services de paiement de prouver que l'opération litigieuse « *a été authentifiée, dûment enregistrée et comptabilisée et qu'elle n'a pas été affectée par une déficience technique ou autre* ». L'alinéa 2 ajoute que l'utilisation de l'instrument de paiement « *ne suffit pas nécessairement en tant que telle à prouver que l'opération a été autorisée par le payeur ou que celui-ci n'a pas satisfait intentionnellement ou par négligence grave aux obligations lui incombant en la matière* ». Il ressort de cette disposition que la charge de la preuve de la fraude ou de la négligence grave appartient entièrement au prestataire de services de paiement. Une telle position a été confirmée par la Cour de cassation, laquelle précise que cette preuve ne peut se déduire du seul fait que l'instrument de paiement ou les données personnelles qui lui sont liées auraient été effectivement utilisés[39].

---

[34] C. consom., art. L. 612-3 ; V. Cass. civ. 2e, 9 juin 2022, n° 19-21798, *Bull. civ.* II ; *JCP E* 2022, act. n° 591 ; *Contrats conc. consom.* 2022, comm. n° 147, obs. S. Bernheim-Desvaux ; *Procédures* 2022, comm. n° 194, obs. Y. Strickler.

[35] C. consom., art. R. 612-4, 1°.

[36] C. consom., art. L. 613-1.

[37] Un tel rappel est déjà formulé dans l'avis rendu par le médiateur au sein duquel il doit indiquer que la solution émise « *peut être différente de la décision qui sera rendue par un juge* », V. C. consom., art. R. 612-4, 3°.

[38] A. Danis-Fatôme, « Paiement à distance et preuve de la négligence grave de l'utilisateur d'un service de paiement : une nouvelle probatio diabolica ? », *RDC* 2017/2, p. 270 *sq.*

[39] Cass. com., 18 janv. 2017, n° 15-18102, *Bull. civ.* IV ; *Banque et droit* mars-avr. 2017, n° 172, p. 32-33, obs. Th. Bonneau ; *RTD com.* 2017, p. 154 *sq.*, obs. D. Legeais ; *RD bancaire et fin.* mars-avr. 2017, comm. n° 44, note Th. Samin et S. Torck ; *Gaz. Pal.* 13 juin 2017, p. 55-56, note M. Roussille ; *JCP G* 2017, 241, note J. Lasserre Capdeville ; *JCP E* 2017, 1122, note K. Rodriguez ; *RD bancaire et fin.* mai-juin 2019, dossier n° 28, K. Rodriguez.

En conséquence, il appartient au banquier de démontrer que l'opération a été correctement réalisée et qu'elle n'a pas subi de déficience technique « *ou autre* » au moment des faits[40]. Hormis l'imprécision de la formule, une telle preuve est difficile sinon impossible à rapporter car cela revient à prouver un fait n'étant pas survenu, c'est-à-dire l'absence de déficience technique des systèmes informatiques de la banque. De surcroît, le banquier n'a pas la possibilité d'accéder à la boîte de messagerie de son client afin de vérifier l'existence de l'e-mail de *phishing*, ni d'obtenir de son opérateur un relevé de la liste des mails reçus. Or, les seuls moyens dont dispose le banquier pour se ménager une preuve reposent exactement sur l'instrument de paiement et les données de sécurité personnalisées attachées à celui-ci. Pour pallier une telle difficulté, il ne reste qu'au banquier à rechercher l'aveu du client quant à sa négligence grave et à fournir des éléments de preuve complémentaires.

13. La nécessaire recherche de preuves complémentaires par le banquier. – Au regard des difficultés rencontrées pour démontrer la négligence grave voire l'intention frauduleuse de son client, le banquier doit rechercher des preuves complémentaires. Il se déduit de cette recherche une présomption selon laquelle le fraudeur n'aurait pas pu réaliser l'opération de paiement litigieuse sans la divulgation d'informations confidentielles, à savoir les données de sécurité personnalisées, par le client à ce dernier[41]. Néanmoins, et à titre d'exemple, le seul fait qu'une carte bancaire ait été utilisée par un tiers avec composition du code confidentiel ne peut suffire à constituer la preuve d'une faute lourde de son titulaire[42].

En revanche, et même s'il est rare en pratique, l'aveu de l'utilisateur du service de paiement concernant sa légèreté blâmable est un élément probant. Celui-ci peut apparaître dans les courriers échangés entre le banquier et son client ou dans le procès-verbal résultant du dépôt de plainte du client à la suite de la fraude constatée. En outre, il est nécessaire que le banquier maîtrise davantage les risques juridiques d'une éventuelle fraude en renforçant ses moyens de preuve. S'il aura certes des difficultés à prouver l'absence de déficience technique, il serait opportun qu'il puisse fournir un tableau chronologique des transactions réalisées avec toutes les explications afférentes[43]. Cela lui permettra notamment de démontrer que les différentes étapes du processus d'authentification forte ont bien été respectées et que seul un défaut de protection de la sécurité des données de sécurité personnalisées émanant de son client est survenu.

14. Conclusion. – La maîtrise des risques juridiques tend à se renforcer, tant pour le client que pour le banquier. L'objectif principal est de juguler la fraude aux moyens de paiement, laquelle se développe avec les paiements à distance. Au regard de la réglementation applicable, la responsabilité du banquier est fréquemment engagée quand bien même il n'a souvent commis aucune faute. Il semble finalement supporter le risque technologique alors que le rôle de

[40] Cass. com., 12 nov. 2020, n° 19-12112, *Bull. civ.* IV ; *Gaz. Pal.* 19 janv. 2021, p. 16 *sq.*, note J. Lasserre Capdeville ; *Gaz. Pal.* 2 févr. 2021, p. 52 *sq.*, note C. Houin-Bressand ; *RD bancaire et fin.* mai-juin 2021, comm. n° 49, obs. Th. Samin et S. Torck ; *J.-Cl. Droit bancaire et financier,* Synthèse n° 20, par D. Legeais.
[41] A. Maymont, « Les présomptions en droit bancaire et financier : un mécanisme probatoire défavorable au banquier », *in Les présomptions, Les artifices du droit (III)*, dir. A.-B. Caire, LGDJ, 2020, p. 157 *sq.*, spéc. n° 11.
[42] Cass. com., 2 oct. 2007, n° 05-19899, *Bull. civ.* IV ; *D.* 2008, p. 454 *sq.*, note A. Boujeka ; *RD bancaire et fin.* nov.-déc. 2007, comm. n° 206, note F.-J. Crédot et Th. Samin et comm. n° 234, note E. A. Caprioli ; *Contrats conc. consom.* 2018, comm. n° 26, obs. G. Raymond. – Sur la caractérisation d'un cas de faute lourde, v. Cass. com., 16 oct. 2012, n° 11-19981, *Bull. civ.* IV ; *D.* 2012, p. 2508, obs. X. Delpech ; *Gaz. Pal.* 13 avr. 2013, p. 17-18, note A.-C. Rouaud ; *JCP E* 2012, 1680, note S. Piédelièvre ; *D.* 2013, p. 407 *sq.*, note J. Lasserre Capdeville.
[43] K. Magnier-Merran, « Des risques liés à certains paiements frauduleux : la banque tenue à l'impossible ? », *RD bancaire et fin.* janv.-févr. 2021, dossier n° 4, spéc. n° 11.

l'utilisateur ne doit pas être négligé[44]. En effet, chaque procès est différent et doit amener les juges à intervenir au cas par cas selon les circonstances de l'espèce. Si ce type de litige peut affecter certains clients, il n'a pas été détecté de litiges sériels, ce qui conforterait l'absence de déficience technique systémique au sein des établissements. En tout état de cause, un basculement paraît s'opérer d'une fraude dite « *technologique* » vers une fraude dite de « *manipulation* »[45]. Plus que le facteur technologique, la vigilance des parties pourra certainement permettre d'atténuer plus encore la fraude en matière de paiement.

[44] N. Kilgus, « Authentification forte et preuve de la négligence grave de l'utilisateur d'un instrument de paiement », *op. cit.,* p. 50.
[45] G. Nedelec, « Paiements : la fraude recule, mais change de nature », *Les Echos* 25 juill. 2022, p. 21 ; OSMP, *op. cit.,* p. 5-6.