COUR DE CASSATION

RAPPORT DE M. CALLOCH, CONSEILLER

Arrêt n° 630 du 10 décembre 2025 (FS-B) – Chambre commerciale financière et économique

Pourvoi n° 24-20.778

Décision attaquée : 20 mars 2023 du tribunal judiciaire de Paris

La société RJSAM
C/
La banque CIC [Adresse 3]

_____

1 - Rappel des faits et de la procédure

Le 5 août 2021, la société RJSAM représentée par sa gérante, Mme [G], a effectué par téléphone une réservation d'une chambre dans un hôtel situé en Italie pour la période du 8 au 15 août 2021 et a communiqué son numéro de carte bancaire ainsi que son code afin de payer la somme de 1 890 euros. Arrivée sur place, il a été indiqué à Mme [G] qu'aucune chambre n'était disponible et l'hôtelier a refusé de rembourser le montant débité.

Mme [G] ès qualité de gérante de la société RJSAM a formé opposition à la carte le 9 août 2021 et a exigé de sa banque, la société banque CIC [Adresse 3] (la banque), le remboursement du montant prélevé sur son compte.

Le 14 novembre 2022, Mme [G] ès qualité de gérante de la société RJSAM a attrait par voie de requête la banque devant le tribunal judiciaire de Paris en paiement de la somme de 1 890 euros, outre 1 000 euros au titre de dommages et intérêts.

Le 20 mars 2023, le tribunal a rejeté l'intégralité des demandes.

C'est la décision attaquée.

2 - Exposé du moyen

La société RJSAM reproche au jugement de rejeter l'intégralité de ses demandes alors :

1°) qu'il résulte des articles L. 133-3, L. 133-6, L. 133-7 et L. 133-18 du code de monétaire et financier que la communication, par téléphone, du numéro de carte bancaire et de son cryptogramme, aux fins de réservation d'une chambre d'hôtel, ne constitue pas un ordre de paiement autorisé au prestataire de service de paiement ; qu'en retenant le contraire, le tribunal a méconnu les textes susvisés ;

2°) qu'il appartenait au tribunal d'examiner si le prestataire de services de paiement établissait que le consentement à l'opération avait été donné sous la forme qui aurait été convenue entre lui et sa cliente, conformément à l'article L. 133-7 du code monétaire et financier ; qu'en s'abstenant de le faire, le tribunal a privé sa décision de base légale au regard de ce texte ;

3°) qu'il résulte des articles L. 133-18, L. 133-19, L. 133-23 et L. 133-24 du code monétaire et financier que s'il appartient à l'utilisateur de services de paiement de prendre toute mesure raisonnable pour préserver la sécurité de ses dispositifs de sécurité personnalisés et d'informer sans tarder son prestataire de tels services de toute utilisation non autorisée de l'instrument de paiement ou des données qui lui sont liées, c'est à ce prestataire qu'il incombe de rapporter la preuve que l'utilisateur, qui nie avoir autorisé une opération de paiement, a agi frauduleusement ou n'a pas satisfait intentionnellement ou par négligence grave à ses obligations ; qu'en se bornant en l'espèce à relever qu' "il n'apparaît pas sérieusement contestable que la requérante a spontanément communiqué à l'hôtelier son numéro de carte bancaire et le cryptogramme de sécurité. Ainsi les dispositions précitées de l'article L. 133-18 du code monétaire et financier ne sauraient aucunement recevoir application dès lors qu'il n'y a pas eu, comme le soutient à tort, Mme [K] [G] épouse [I], d'opération non autorisée ; qu'il n'y a eu aucune fraude dans le paiement par carte
bancaire " sans rechercher, comme il lui incombait, si elle, qui niait avoir autorisé l'opération de paiement, aurait agi frauduleusement ou n'aurait pas satisfait intentionnellement ou par négligence grave à ses obligations, le tribunal a privé sa décision de base légale au regard des textes susvisés ;

4°) qu' il résulte des articles L. 133-19, V du code monétaire et financier dans leur rédaction issue de l'ordonnance n° 2017-1252 du 9 août 2017 que, sauf agissement frauduleux de sa part, le payeur ne supporte aucune conséquence financière si l'opération de paiement non autorisée a été effectuée sans que le prestataire de services de paiement du payeur n'exige une authentification forte du payeur prévue par le second de ces textes ; qu'il résulte en outre de l'article 34, VIII, 3°, de l'ordonnance n° 2017-1252 du 9 août 2017, que l'article L. 133-44, auquel renvoie l'article L. 133-19, est entré en vigueur le 14 septembre 2019, dix-huit mois après l'entrée en vigueur du

règlement délégué (UE) 2018/389 de la Commission du 27 novembre 2017 complétant la directive (UE) 2015/2366 par des normes techniques de réglementation relatives à l'authentification forte du client et à des normes ouvertes communes et sécurisées de communication ; qu'en l'espèce, le tribunal a estimé qu'
"il n'apparaît pas sérieusement contestable que la requérante a spontanément communiqué à l'hôtelier son numéro de carte bancaire et le cryptogramme de sécurité. Ainsi les dispositions précitées de l'article L. 133-18 du code monétaire et financier ne sauraient aucunement recevoir application dès lors qu'il n'y a pas eu, comme le soutient à tort, Mme [K] [G] épouse [I], d'opération non autorisée ; qu'il n'y a eu aucune fraude dans le paiement par carte bancaire " ; qu'en statuant ainsi, sans rechercher, comme il lui incombait, si l'opération de paiement litigieuse n'avait pas été exécutée sans que la banque exige l'authentification forte du payeur, le tribunal a privé sa décision de base légale au regard des textes susvisés.

3 - Identification du ou des points de droit faisant difficulté à juger

Le pourvoi pose la question du caractère autorisé d'une opération de paiement initiée par le payeur donnant un ordre de paiement par l'intermédiaire du bénéficiaire à qui il a transmis par téléphone le numéro de sa carte bancaire et le cryptogramme y étant associé ainsi que l'obligation pour l'établissement de crédit d'exiger dans cette hypothèse l'authentification forte.

4 - Discussion citant les références de jurisprudence et de doctrine

4.1. Opération de paiement non autorisée et consentement au paiement donné par l'intermédiaire du bénéficiaire

On sait que notre chambre, par deux arrêts publiés récents, a repris la règle posée par la CJUE dans l'arrêt du 16 mars 2023, Beobank (C-351/21) selon laquelle le régime de responsabilité en matière d'opérations de paiement non autorisées prévu par le code monétaire et financier transposant la directive 2007/64/CE du Parlement européen et du Conseil du 13 novembre 2007 (directive DSP 1) était seul applicable, à l'exclusion de tout régime alternatif de responsabilité résultant du droit national (Com., 27 mars 2024, n° 22-21.200, publié au bulletin ; Com., 2 mai 2024, n° 22-18074, publié au bulletin).[1]

Le pourvoi affirme que les dispositions du code monétaire et financier relatives à la responsabilité du prestataire de services en cas d'opération de paiement non autorisée devaient s'appliquer au litige, et ce alors que le tribunal les avait écartées au motif que l'opération litigieuse ne constituait pas une opération non autorisée.

[1]. B. Michalet, A. Moisson, M. Tardieu Confavreux, contentieux des opérations de paiement : l'exclusivité du régime des articles L. 133-18 et suivants du code monétaire et financier , applications et perspectives. Revue de droit bancaire et financier n° 3, Mai-juin 2024, étude 5 ; J. Lassere Capdeville, nouvelles précisions sur le droit applicable aux opérations de paiement non autorisées, JCP E, n° 24, 4 juillet 2024, page 47 ; C. Hélaine, responsabilité du prestataire de services de paiement : le triomphe du droit spécial, Dalloz actualité 3 avril 2024.

L'article L. 133-6 du code monétaire et financier dispose qu'une opération de paiement est autorisée si le payeur a donné son consentement à son exécution. L'article L. 133-7 suivant précise que « le consentement est donné sous la forme convenue entre le payeur et son prestataire de services de paiement » et qu'en l'absence d'un tel consentement l'opération de paiement « est réputée non autorisée ».

En application de ces deux textes, notre chambre a été amenée à définir l'opération de paiement non autorisée comme l'opération pour laquelle le payeur n'avait pas donné son consentement sous la forme convenue avec le prestataire, ce consentement devant porter notamment sur l'identité du bénéficiaire (Com. 1er juin 2023, n° 21-19289 B, à propos d'un numéro d'IBAN falsifié dans un ordre de virement)[2]ou sur le montant de l'opération (Com. 30 novembre 2022, n° 21-17.614 B).

Elle a admis qu'un ordre de virement pouvait être donné oralement dès lors que les conditions générales de la convention de compte prévoyaient la possibilité de déroger à la règle d'un ordre écrit et qu'il était établi que ce type d'ordres avait déjà été utilisé par le payeur (Com., 2 mai 2024, n° 22-17.233, publié au bulletin).

Transposant la directive (UE) 2015/2366 du Parlement européen et du Conseil, l'article L. 133-3 II b du code monétaire et financier dispose qu'une opération de paiement peut être initiée par le payeur mais aussi « *par le payeur, qui donne un ordre de paiement par l'intermédiaire du bénéficiaire qui, après avoir recueilli l'ordre de paiement du payer, le transmet au prestataire de services de paiement du payeur, le cas échéant, par l'intermédiaire de son propre prestataire de services de paiement* »
L'article L. 133-7 a, de même, expressément prévu que le consentement à l'opération pouvait être donné non seulement par le payeur, mais aussi « *par l'intermédiaire du bénéficiaire ou d'un prestataire de services de paiement fournissant un service d'initiation de paiement* » (article L. 133-7, alinéa 2 du code monétaire et financier)

L'article L. 133-8 II du même code prévoit que lorsque l'opération de paiement est ainsi initiée par le payeur donnant un ordre de paiement par l'intermédiaire du bénéficiaire, le payeur ne peut révoquer l'ordre de paiement après avoir transmis l'ordre de paiement au bénéficiaire ou donné son consentement à l'exécution de l'opération de paiement au bénéficiaire.

Ainsi que le rappelle un commentateur «*L'irrévocabilité interviendra donc instantanément. Une révocation entre le moment où le titulaire a transmis l'ordre de paiement au bénéficiaire et le moment ou cet ordre est transmis par le bénéficiaire au banquier du titulaire de la carte pour encaissement est donc inopérante, sauf cas d'opposition justifiée* » (*J. F Riffard, JCl Droit bancaire et financier. Fas.270 : paiement par carte bancaire § 58*)

La directive (UE) 2015/2366 du Parlement européen et du Conseil (DSP2) prévoit en son article 75 l'hypothèse de l'opération de paiement initiée par l'intermédiaire du bénéficiaire lui-même dont le montant n'est pas encore exactement déterminé. Il s'agit

[2]. J. Lasserre Capdeville, la substitution frauduleuse du RIB, Revue de droit bancaire et financier n° 3, mai-juin 2024, alerte 50.

là notamment de l'hypothèse de l'espèce, à savoir la communication de ses coordonnées par le payeur dans le cadre d'une réservation d'hôtel.

Le considérant 75 de la directive est sur ce point éclairant :

La présente directive vise à renforcer la protection des consommateurs dans le cas d'opérations de paiement liées à une carte où le montant exact de l'opération n'est pas connu au moment où le payeur donne son consentement à l'exécution de l'opération de paiement, par exemple dans les stations-service automatiques ou dans le cas de contrats de location de voiture ou de réservations d'hôtel. Le prestataire de services de paiement du payeur devrait pouvoir bloquer des fonds sur le compte de paiement du payeur uniquement si celui-ci a donné son consentement quant au montant exact des fonds à bloquer et ces fonds devraient être débloqués sans retard injustifié après réception des informations sur le montant exact de l'opération de paiement et au plus tard immédiatement après réception de l'ordre de paiement.

Cette volonté de protection du payeur est traduite par l'article 75 de la directive :

Article 75

Opérations de paiement dont le montant n'est pas connu à l'avance

1. Lorsqu'une opération de paiement est initiée par ou par l'intermédiaire du bénéficiaire dans le cadre d'une opération de paiement liée à une carte et que le montant exact n'est pas connu au moment où le payeur donne son consentement à l'exécution de l'opération de paiement, le prestataire de services de paiement du payeur peut bloquer des fonds sur le compte de paiement du payeur uniquement si celui-ci a donné son consentement quant au montant exact des fonds à bloquer.

2.Le prestataire de services de paiement du payeur débloque les fonds bloqués sur le compte de paiement du payeur au titre au paragraphe 1 sans retard injustifié après réception des informations sur le montant exact de l'opération de paiement et au plus tard immédiatement après réception de l'ordre de paiement.

Cette disposition a été transposée à l'article L. 133-25 du code monétaire et financier :

Article L133-25

I. – Le payeur a droit au remboursement par son prestataire de services de paiement d'une opération de paiement autorisée, ordonnée par le bénéficiaire ou par le payeur qui donne un ordre de paiement par l'intermédiaire du bénéficiaire, si l'autorisation donnée n'indiquait pas le montant exact de l'opération de paiement et si le montant de l'opération dépassait le montant auquel le payeur pouvait raisonnablement s'attendre en tenant compte du profil de ses dépenses passées, des conditions prévues par son contrat-cadre et des circonstances propres à l'opération.

A la demande du prestataire de services de paiement, le payeur fournit tous éléments relatifs au remboursement demandé.

II. – Dans le cas où le montant de l'opération dépasse le montant auquel le payeur pouvait raisonnablement s'attendre conformément au I, le payeur ne peut invoquer des raisons liées à une opération de change si le taux de change de référence convenu avec son prestataire de services de paiement a été appliqué.

III. – Le payeur présente sa demande de remboursement avant l'expiration d'une période de huit semaines à compter de la date à laquelle les fonds ont été débités. Dans un délai de dix jours ouvrables suivant la réception de la demande de remboursement, le prestataire de services de paiement soit rembourse le montant total de l'opération de paiement, soit justifie son refus de rembourser, en indiquant la possibilité de recourir à la procédure de médiation mentionnée à l'article L. 316-1.

IV. – Le remboursement prévu dans la présente section correspond au montant total de l'opération de paiement exécutée. La date de valeur à laquelle le compte de paiement du payeur est crédité n'est pas postérieure à la date à laquelle il a été débité.

Commentant cet article, un auteur expose que « *si cette disposition légale peut éventuellement concerner des réservations à distance (véhicule, chambre d'hôtel, etc.), on peut penser que son application demeurera, en réalité, peu fréquente dans ces hypothèses. En effet, dans la majorité des cas de réservation, l'intéressé aura une connaissance approximative du montant global du paiement. Par exemple, à l'égard d'une chambre d'hôtel, il connaitra généralement le prix de la chambre pour une nuit* ». (J. Lasserre Capdvielle et al. Droit bancaire, n° 1579, Précis Dalloz, 3e édition).

4.2. Examen des griefs.

4.2.1. Première à troisième branches du moyen : nature d'un ordre de paiement sous forme de communication à un tiers du numéro de carte bancaire et du cryptogramme (ou code EMV).

1ère branche du moyen : opération de paiement autorisée et communication par téléphone du numéro de carte bancaire au bénéficiaire.

La société RJSAM n'invoque pas un dépassement du montant escompté, ce montant étant au demeurant déjà défini dans la demande d'autorisation de paiement adressée par l'hôtelier, et donc les dispositions de l'article L. 133-25 du code monétaire et financier, mais soutient que la communication par téléphone du numéro d'une carte de paiement et de son cryptogramme ne constitue pas une opération de paiement autorisée au sens du code monétaire et financier.

Le jugement attaqué retient qu' « *il n'apparaît pas sérieusement contestable que la requérante a spontanément communiqué à l'hôtelier son numéro de carte bancaire et le cryptogramme de sécurité* » et en déduit « *qu'il n'y a pas eu (.....) d'opération non autorisée.* »

Ce jugement a ainsi constaté que la société RJSAM avait donné l'ordre de paiement par l'intermédiaire du bénéficiaire, en adressant à celui-ci le numéro de sa carte bancaire et le cryptogramme de sécurité y étant lié.

Ainsi qu'il a été rappelé plus haut, l'article L. 133-7 du code monétaire et financier transposant la directive (UE) 2015/2366 du Parlement européen et du Conseil prévoit expressément la possibilité que le consentement à l'opération de paiement puisse être donné par l'intermédiaire du bénéficiaire.

Le consentement du payeur résulte de cette transmission au bénéficiaire des données de l'instrument de paiement et des données personnalisées de sécurité que constitue le cryptogramme, opération relevant des paiements dits « MOTO » selon le glossaire édité par l'Observatoire de la sécurité des moyens de paiement et figurant en annexe 1 du plan de sécurisation des paiements par carte à distance du 10 juin 2024 (consultable sur son site internet).

Ce consentement ainsi donné, l'ordre de paiement devient irrévocable dès lors que le payeur a transmis l'ordre de paiement au bénéficiaire ou a donné son consentement à l'exécution de l'opération au paiement au bénéficiaire (article L. 133-8 II du code monétaire et financier)

En raison de ce caractère irrévocable, le payeur ne peut demander le remboursement de l'ordre de paiement que dans la seule hypothèse, comme on l'a vu, où l'autorisation donnée n'indiquait pas le montant exact de l'opération de paiement et où, au final, le montant de l'opération « dépassait le montant auquel le payeur pouvait raisonnablement s'attendre ».

En l'espèce, il résulte de la demande de virement adressée par l'hôtelier et accompagnée du détail des sommes dues, que la société RJSAM avait connaissance de la somme exacte à débiter.

C'est donc conformément aux dispositions du code monétaire et financier que le tribunal a considéré que la société RJSAM avait autorisé l'opération de paiement en adressant au bénéficiaire les informations permettant à celui-ci de l'initier.

Le consentement à l'opération de paiement ayant ainsi été jugé caractérisé, et cette opération étant à bon droit qualifiée d'opération autorisée, il ne peut être reproché au tribunal d'avoir violé les dispositions du code monétaire et financier.

La première branche du moyen apparaît de ce fait manifestement non fondée.

Deuxième branche du moyen : consentement donné dans la forme convenue entre les parties.

On sait que l'article L. 133-7 du code monétaire et financier dispose que le consentement à une opération de paiement « *est donné sous la forme convenue entre le payeur et son prestataire de services de paiement* » et « *qu'en l'absence d'un tel consentement, l'opération ou la série d'opération de paiement est réputée non autorisée.*»

Dans sa deuxième branche, le moyen reproche au jugement de ne pas avoir recherché si la société RJSAM, en transmettant à l'hôtelier le numéro de sa carte bancaire et le

cryptogramme y figurant, avait donné son consentement à l'opération sous la forme convenue avec sa banque.

Cette nécessité d'un consentement « *donné sous la forme convenue entre le payeur et son prestataire de services de paiement* » pose difficulté dans l'hypothèse où ce consentement a été donné comme en l'espèce par l'intermédiaire du bénéficiaire lui-même.

Dans leur ouvrage « Instruments de crédit et de paiement »[3], les auteurs indiquent sur ce point :

La forme du consentement est librement convenue entre le payeur et son prestataire ; un arrêté du 29 juillet 2009 (art. 2-2-c) précise que la convention la mentionne ainsi que celle du retrait du consentement. L'utilisation d'un dispositif de sécurité personnalisé (devenu « données de sécurité personnalisées »), destiné à authentifier l'auteur (v. infra, la frappe du code secret de la carte bancaire, ou la composition d'un code d'accès à ses comptes personnels sur internet), peut jouer ainsi un rôle déterminant dans l'expression de volonté du donneur d'ordre.

Selon ces mêmes auteurs, les conventions types habituelles proposées par les prestataires de services de paiement prévoient comme forme du consentement dans l'hypothèse d'un ordre transmis au bénéficiaire « *la frappe du code confidentiel sur le clavier de l'équipement électronique du bénéficiaire ou la signature de la facture (...) d'une part, la communication à distance des données liées à l'utilisation de la carte (numéro facial et code à trois chiffres au dos de la carte, dit code « EMV3) d'autre part* » (R. Bonhomme et al, ouvrage cité note 4, 387).

Antérieurement à la transposition de la directive (UE) 2015/2366 du Parlement européen et du Conseil, la première chambre civile, dans un arrêt du 19 octobre 1999 rendu dans des circonstances de fait similaires (coordonnées d'une carte bancaire communiquées à un hôtelier pour assurer la réservation d'une chambre) avait déjà considéré qu'une cliente « avait autorisé le débit » de cette carte en cas d'annulation de la réservation (1re Civ, 19 octobre 1999, n° 97-10.556, publié). Mais cette décision ne concernait que les rapports entre la cliente et l'hôtelier.

Dans les rapports entre le payeur et la banque, notre chambre avait à plusieurs reprises statué sur les conséquences de la communication des coordonnées d'une carte bancaire et de son cryptogramme à un hôtelier afin de garantir une réservation avant l'entrée en vigueur de l'ordonnance n° 2009-866 du 15 juillet 2009 transposant la directive DSP 2. Elle avait considéré que la communication à distance de ces données n'établissait pas l'existence d'un mandat donné à la banque de payer la somme prélevée à la demande de l'hôtelier (Com., 24 mars 2009, n° 08-12.025 ; Com., 12 décembre 2006, n° 05-15.481, publié).

L'examen de ces décisions rendues au visa des dispositions abrogées du code monétaire et financier relatives aux cartes de paiement permet de constater cependant que les circonstances de fait étaient différentes du présent litige.

[3]. R. Bonhomme, M. Rousille et al., Instrurments de crédit et de paiement, 359, LGDJ, 14ème édition

Dans la première affaire, le payeur avait expressément indiqué à l'hôtelier que la communication des données de sa carte n'avait été effectuée que pour garantir la réservation, sur un formulaire précisant que cette communication ne donnerait lieu à aucun débit (n° 08-12.025). Dans la seconde (05-15481), non seulement la banque elle-même avait reconnu que le virement avait été effectué suite à une erreur de l'hôtelier, mais surtout que le payeur s'était contenté de donner le numéro de sa carte, sans communiquer le code confidentiel ni signer d'autorisation.

Ces deux décisions, appliquant les règles civiles du dépôt, sont en conséquence sans incidence sur le constat fait par le jugement attaqué selon lequel, conformément aux dispositions du code monétaire et financier, la société RJSAM avait donné un ordre de paiement irrévocable par l'intermédiaire du bénéficiaire pour un montant déterminé et en paiement d'une prestation, la circonstance selon laquelle cette prestation n'a pas été finalement fournie par ce bénéficiaire étant sans incidence sur le caractère autorisé de l'ordre de paiement.

La société RJSAM soutient qu'il appartenait au tribunal d'examiner si le prestataire de services de paiement « établissait que le consentement de l'opération avait été donné sous la forme qui aurait été convenu entre lui et sa cliente ».

Il apparaît cependant de la lecture de la décision que la société RJSAM n'a pas contesté devant le tribunal que la convention par elle signée avec la banque autorisait, conformément aux conventions types, que l'ordre de paiement soit transmis au bénéficiaire en communiquant à distance des données liées à l'utilisation de la carte (numéro facial et code à trois chiffres au dos de la carte, dit code « EMV3).

Le grief est donc nouveau, mélangé de fait et de droit, et partant irrecevable.

Troisième branche du moyen.

La troisième branche apparaît, elle, **inopérante**, invoquant les dispositions des articles L. 133-18, L 133-19 et L. 133-23 inapplicables au litige dès lors que l'opération de paiement constitue une opération de paiement autorisée.

Les griefs ne sont donc manifestement pas de nature à entraîner la cassation et il est proposé de les rejeter par une décision non spécialement motivée.

4.2.2. Quatrième branche : exigence d'une identification forte.

Dans une quatrième branche, le pourvoi invoque les dispositions de l'article L. 133-19, V du code monétaire et financier et soutient que le tribunal a privé la décision de base légale en ne recherchant pas, comme il lui incombait, si l'opération litigieuse n'avait pas été exécutée sans que la banque exige l'identification forte du payeur.

On rappellera que notre chambre, dans un arrêt du 30 août 2023 (Com. 30 août 2023, n° 22-11707,)[4] a posé le principe que, sauf agissement frauduleux de sa part, le payeur ne supporte aucune conséquence financière si l'opération de paiement non autorisée a été effectuée sans que le prestataire de services de paiement n'exige une authentification forte prévue par l'article L. 133-4 du code monétaire et financier.

La banque soulève l'irrecevabilité de ce grief, Mme [G] n'ayant jamais invoqué dans ses conclusions l'application de l'article L. 133-19 V du code monétaire et financier. Il convient cependant de constater que dans ses conclusions, Mme [G] indiquait : « *Il appartenait à la banque de mettre en oeuvre un système de sécurité performant applicable au paiement à l'étranger (par exemple : envoi d'un SMS pour autoriser un tel paiement.....), ce qu'elle n'a pas fait* », mettant ainsi dans les débats la question de l'utilisation de l'identification forte du payeur, peu important qu'elle la considère de manière erronée comme réservée aux paiements effectués à l'étranger.

Sur le fond, il convient de rappeler que l'article L. 133-44 du code monétaire et financier que le prestataire de services de paiement n'est tenu d'appliquer l'authentification forte du client que dans trois circonstances, soit lorsque le payeur :
1° Accède à son compte de paiement en ligne;
2° Initie une opération de paiement électronique ;
3° Exécute une opération par le biais d'un moyen de communication à distance, susceptible de comporter un risque de fraude en matière de paiement ou de toute autre utilisation frauduleuse.

Le règlement délégué (UE) 2018/389 de la Commission du 27 novembre 2017 indique dans son considérant 7 que « les exigences relatives à l'authentification forte du client s'appliquent aux paiement initiés par le payeur, que celui-ci soit une personne physique ou une entité juridique ».

Il appartiendra à notre chambre de déterminer d'une part si l'exigence d'une authentification forte s'applique dans l'hypothèse d'un paiement initié par le bénéficiaire et d'autre part si l'appel téléphonique permettant la communication d'un numéro de carte bancaire et de son cryptogramme à un bénéficiaire constitue un « moyen de communication à distance susceptible de comporter un risque de fraude en matière de paiement », et si en conséquence le prestataire de services de paiement était en l'espèce tenu d'exiger du payeur une identification forte.

[4]. C. Hélaine, De l'importance de l'authentification forte en cas d'opération de paiement non autorisée. Dalloz actualité, 28 septembre 2023.