COUR DE CASSATION

INFORMATION relative au rapport du conseiller rapporteur

Le présent rapport a été établi par un magistrat de la Cour de cassation, désigné conseiller rapporteur, en vue d'instruire une affaire (le « pourvoi en cassation ») soumise à la Cour de cassation. Au vu de ce rapport et des autres documents de la procédure, et après en avoir délibéré dans une formation de jugement comportant plusieurs juges, la Cour de cassation a tranché l'affaire par un arrêt, également diffusé sur Judilibre. Ce rapport est un document de travail préparatoire établi, d'abord, à l'intention des magistrats du siège de la Cour appelés à trancher l'affaire. Ces magistrats sont des spécialistes de la question de droit examinée dans le rapport, qui n'a dès lors pas vocation à faire une présentation doctrinale de l'état du droit, mais à procéder à l'analyse de la procédure, des éléments de droit pertinents et des éventuels enjeux juridiques de l'affaire. Conformément au principe du contradictoire, ce document est également communiqué aux parties ou à leurs avocats, ainsi qu'à l'avocat général. Enfin, ce rapport fournit une analyse à l'issue de laquelle le conseiller rapporteur ne donne pas son avis, lequel est soumis au secret du délibéré. Le rapport est donc toujours complété par deux autres documents établis par le rapporteur à l'intention des autres magistrats de la formation de jugement : une note d'avis et le ou les projets d'arrêts qu'il a préparés. Ces documents ne sont pas accessibles sur Judilibre.

N° Z2517510		CO	
Décision attaquée : 28 mai 2025 de la cour d'appel de Paris			

la société Eleco Panacol - EFD C/ la société HSBC Continental Europe _____	
rapporteur : Pierre Calloch	**RAPPORT**

TABLEAU SYNOPTIQUE DU RAPPORTEUR	
Identification du ou des points de droit à juger	- Obligation pour le prestataire de services de paiement d'exiger une authentification forte. - Caractère exclusif de la responsabilité du prestataire de services de paiement en cas d'opération non autorisée.

Formation proposée	☒ formation restreinte
En cas de publication de l'arrêt à rendre, intérêt de la diffusion du rapport sur Judilibre	☒ Non

Nombre de projets d'arrêt préparés	☒ un projet d'arrêt

1 - Rappel des faits et de la procédure

Le 16 décembre 2019, Mme [B], assistante administrative du président de la société Eleco, a été contactée téléphoniquement par un interlocuteur se faisant passer pour un avocat et lui indiquant avoir été désigné par le président pour effectuer une offre publique d'achat confidentielle et urgente et lui demandant en conséquence d'effectuer un virement d'un montant de 383 268, 37 euros au bénéfice d'un compte situé en Hongrie.

Mme [B] a téléchargé sur le site de la société HSBC Continental Europe (la banque) dans les livres de laquelle la société avait ouvert un compte courant un ordre de virement qu'elle a adressé par courriel à son interlocuteur. Celui ci lui a renvoyé avec la signature imitée du président de la société.

Le 17 décembre 2019, Mme [B] a faxé cet ordre de virement portant fausse signature à la banque, qui l'a exécuté dans la journée.

Découvrant le même jour avoir été victime d'une « fraude au président », la société a contacté la banque a pu récupérer seulement la somme de 271,19 euros selon la procédure de retour de fonds.

La société a déposé plainte pour escroquerie et a assigné la banque devant le tribunal de commerce de Paris en restitution de la somme débitée en exécution de l'ordre de virement et non restituée.

Le 9 mars 2023, le tribunal a condamné la banque à payer à la société la somme de 382 997, 18 euros.

Le 28 mai 2025, la cour d'appel de Paris a infirmé cette décision et statuant à nouveau a rejeté l'intégralité des demandes formées par la société.

C'est la décision attaquée par un pourvoi de la société Eleco Panacol - EFD **.**

Procédure devant la Cour de cassation

Pourvoi	N° Z2517510 Du 28 juillet 2025
Mémoire ampliatif	Déposé le 1 décembre 2025 (article 700 CPC : 5 000 euros).
Mémoires en défense et pourvois incidents	- Mémoire en défense de la société HSBC Continental Europe: déposé le 30 janvier 2026 (article 700 CPC : 5 000 euros).

La procédure semble régulière et l'affaire en état d'être jugée.

2 - Exposé des moyens

2.1 - Premier moyen

La société fait grief à l'arrêt de rejeter l'ensemble de ses demandes dirigées contre la banque, alors :

« 1°/ que lorsqu'un utilisateur de services de paiement nie avoir autorisé une opération de paiement qui a été exécutée, il incombe à son prestataire de services de paiement de prouver que l'opération en question a été authentifiée, dûment enregistrée et comptabilisée et qu'elle n'a pas été affectée par une déficience technique ou autre ; qu'à défaut de rapporter cette preuve, le prestataire ne peut faire supporter à l'utilisateur les pertes occasionnées par l'opération au motif qu'elle aurait été rendue possible par un manquement de cet utilisateur, intentionnel ou par négligence grave, aux obligations mentionnées aux articles L. 133-16 et L 133-17 du code monétaire et financier ; qu'au cas d'espèce, la cour ayant retenu que le virement litigieux du 17 décembre 2019 n'avait pas été effectué au moyen de l'utilisation de la clé numérique « 3S Key » prévue au dispositif de sécurité personnalisé auquel la société Eleco avait souscrit le 10 mars 2017, il en résultait que l'opération n'avait pas été authentifiée comme elle aurait dû l'être selon les stipulations contractuelles, en sorte que la banque ne pouvait se dégager de sa responsabilité en invoquant un manquement par la société utilisatrice aux obligations susvisées ; qu'en décidant le contraire, elle a violé les articles L. 133-7, L. 133-23 et L. 133-4 du code monétaire et financier, ensemble l'article L. 133-16 du même code, ensemble l'article 1103 du code civil ;

2°/ Que par principe, en cas d'opération de paiement non autorisée signalée par l'utilisateur, le prestataire de services de paiement du payeur doit rembourser au payeur le montant de l'opération non autorisée ; que si l'article L. 133-16 du code monétaire et financier prévoit que dès qu'il reçoit un instrument de paiement, l'utilisateur de services de paiement prend toute mesure raisonnable pour préserver la sécurité de ses données de sécurité personnalisées et qu'il utilise l'instrument de paiement conformément aux conditions régissant sa délivrance et son utilisation qui doivent être objectives, non discriminatoires et proportionnées, ce texte ne crée pas en lui-même une cause d'exonération du prestataire de services de paiement en cas d'opération de paiement non autorisée ; qu'enfin, si, en application de l'article L. 133-19, IV du même code, le payeur supporte toutes 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 aux obligations mentionnées aux articles L. 133-16 et L. 133-17 du même code, cette cause d'exonération suppose que cette opération ait été effectuée à l'aide d'un instrument de paiement doté de données de sécurité personnalisées ; qu'au cas d'espèce, ayant retenu que le virement litigieux du 17 décembre 2019 n'avait pas été effectué au moyen de l'utilisation de la clé numérique « 3S Key » prévue au dispositif de sécurité personnalisé auquel la société Eleco avait souscrit le 10 mars 2017 et qu'en conséquence, les dispositions de l'article L. 133-19, IV susvisé, qui concernent le cas particulier des instruments de paiement dotés d'un dispositif de sécurité personnalisé, n'était pas applicables, la cour d'appel ne pouvait considérer néanmoins que la banque était fondée à s'exonérer en opposant la négligence grave du payeur au seul visa de l'article L. 133-16 susvisé ; qu'en statuant comme elle l'a fait, elle a violé les articles L. 133-18, L. 133-16 et L. 133-19, IV du code monétaire et financier;

3°. Que le prestataire de services de paiement doit appliquer l'authentification forte du client définie au f) de l'article L. 133-4 du code monétaire et financier lorsque le payeur 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 ; qu'au cas d'espèce, à supposer par impossible que nonobstant l'inapplicabilité de l'article L. 133-19, IV du même code, faute d'utilisation d'un instrument de paiement doté d'un dispositif de sécurité personnalisé, la cause d'exonération du prestataire de services de paiement tenant à la négligence grave du payeur au visa de l'article L. 133-16 du même code pût être invoquée, en s'abstenant de rechercher, comme elle y était invitée, si la banque n'avait pas manqué à son obligation d'exiger une authentification forte avant d'exécuter le virement litigieux, ce qui lui interdisait se dégager de sa responsabilité en invoquant une négligence grave de l'utilisateur, la cour d'appel n'a pas donné de base légale à sa décision au regard des articles L. 133-18, L. 133-16, L. 133-44 et L. 133-4 du code monétaire et financier.»

2.2 - Second moyen

La société fait le même grief à l'arrêt, alors :

« 1°/ que dès lors que la responsabilité d'un prestataire de services de paiement est recherchée en raison d'une opération non autorisée ou mal exécutée, seul est applicable le régime de responsabilité défini aux articles L. 133-18 à L. 133-24 du code monétaire et financier, pris en transposition de la directive 2007/64/CE puis de la directive (UE) n° 2015/2366, à l'exclusion de tout régime alternatif de responsabilité résultant du droit national ; qu'au cas d'espèce, en retenant que la société Eleco avait engagé sa responsabilité à l'égard de la banque sur le fondement du droit commun de la responsabilité délictuelle (responsabilité du commettant du fait de son préposé), la cour d'appel a violé les articles L. 133-18 et L. 133-16 du code monétaire et financier, ensemble l'article 1242 du code civil ;

2°/ que la responsabilité du payeur à l'égard du prestataire de services d'investissement tenant à une négligence grave commise par le premier dans le cadre d'une opération de paiement non autorisée, à supposer même qu'elle puisse relever du droit commun, s'inscrit dans leurs rapports contractuels et ne peut être sanctionnée que sur le fondement de la responsabilité contractuelle ; qu'en l'espèce, en retenant que la société Eleco avait engagé sa responsabilité à l'égard de la banque sur le fondement du droit commun de la responsabilité délictuelle (responsabilité du commettant du fait de son préposé), la cour d'appel a violé les articles 1231-1 et 1242 du code civil, ensemble le principe du non-cumul des responsabilité contractuelle et délictuelle. »

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

Responsabilité du prestataire de services de paiement en cas d'opération de paiement résultant d'une « fraude au président » et transmise sans que le prestataire n'exige l'authentification forte. Caractère exclusif des dispositions du code monétaire et financier.

4 - Discussion citant les références de jurisprudence et de doctrine

4.1 - Caractère non autorisé d'une opération de paiement résultant d'un ordre falsifié. L'obligation d'exiger une authentification forte.

4.1.1 La responsabilité du prestataire de services de paiement dans l'hypothèse d'une opération de paiement non autorisée.

On sait que le code monétaire et financier transposant les directives 2007/64/CE du Parlement européen et du Conseil (directive DSP1) et (UE) 2015/2366 du Parlement européen et du conseil du 25 novembre 2015 (directive DSP2) a institué un régime de responsabilité en cas d'opération de paiement non autorisée reposant en substance sur l'obligation de remboursement de ces opérations par le prestataire de services de paiement, sauf pour lui à prouver une fraude ou une négligence grave imputable au payeur.

La question du caractère exclusif de ce régime alors que le droit national se fonde, lui, sur le droit commun de la responsabilité contractuelle, et l'existence d'une obligation de vigilance du prestataire, pour trancher les litiges résultant de l'existence d'ordres de paiement non consentis par le payeur s'est posée, et ce dans un contexte d'une augmentation des escroqueries affectant les moyens de paiement par distance. Le 16 mars 2023, la cinquième chambre de la CJUE a rendu un arrêt en matière de responsabilité du prestataire de services de paiement (arrêt Beobank, 16 mars 2023 C-351-21) affirmant le caractère exclusif du régime de responsabilité des prestataires de services de paiement prévu par la directive en cas d'opération non autorisée ou mal exécutée. Notre chambre a repris son interprétation dans un arrêt du 27 mars 2024 (Com., 27 o mars 2024, n 22-21.200 , publié) rappelant les points 37 et 38 de cet arrêt du 16 mars 2023, Beobank, pour en déduire :

11. Il s'ensuit que, dès lors que la responsabilité d'un prestataire de services de paiement est recherchée en raison d'une opération de paiement non autorisée ou mal exécutée, seul est applicable le régime de responsabilité défini aux articles L. 133-18 à L. 133-24 précités, qui transposent les articles 58, 59 et 60, paragraphe 1, de la directive 2007/64/CE, à l'exclusion de tout régime alternatif de responsabilité résultant du droit national. Notre chambre a réaffirmé depuis dans deux arrêts publiés le caractère exclusif des dispositions du code monétaire et financier dès lors que la responsabilité de la banque était recherchée suite à une opération de paiement non autorisée ou mal exécutée (Com., janvier 2025, n° 23-15.437 , publié, Com. 15 janvier 2025, n° 23-13.579 Com., publié) .

Pour déterminer le régime de responsabilité applicable, le régime prévu par le code monétaire et financier ou le régime de la responsabilité contractuelle de la banque teneur de compte, il convient dès lors de qualifier les opérations litigieuses en opérations non autorisées ou mal exécutées, ou en opérations autorisées. Pour être qualifiée d'opération autorisée, il résulte des dispositions du code monétaire et financier qu'une opération de paiement doit revêtir une double condition cumulative :

1° le consentement doit avoir été donné sous la forme convenue entre le payeur et son prestataire de services de paiement (article L. 133-7, alinéa 1du code monétaire et financier) et donc en utilisant l'instrument de paiement conformément aux dispositions contractuelles. A défaut, l'opération « est réputée non autorisée » (article L. 133-7, alinéa 3).

2° même donné sous la forme convenue, le consentement doit émaner du titulaire de l'instrument de paiement contractuellement déterminé (le payeur) et porter notamment sur tous les éléments de l'ordre, montant et identité du bénéficiaire. Dès lors qu'un tiers est à l'origine de l'ordre de paiement ou a modifié l'un des éléments, le consentement ne peut être considéré comme donné. La Chambre commerciale a ainsi jugé que le payeur devait consentir au montant de l'opération , ou que le virement régulier, mais dont le numéro IBAN du compte bénéficiaire avait été modifié par un tiers à l'insu du payeur, ne constitue pas un ordre de paiement autorisé (Cass., com. 1 er juin 2023, pourvoi n° 21-19.289, publié).

Dès lors que l'opération de paiement est qualifiée de non autorisée, l'article L. 133-18 du code monétaire et financier prévoit l'obligation pour le prestataire de service de paiement l'obligation de rembourser immédiatement le payeur, sauf à démontrer que les pertes résultent d'une fraude de celui-ci ou de négligences graves aux obligations mentionnées aux articles L. 133-16 et L. 133-17 du même code (article L.133-19 IV). Il en résulte qu'une cour d'appel ne peut après avoir relevé que l'opération litigieuse était une opération non autorisée écarter la responsabilité d'une banque au motif que le payeur avait participé du fait de sa négligence à la réalisation de son propre dommage (Com., 4 février 2026, n° 24-22.320).

4.1.2. L'obligation pour le prestataire de services de paiement d'exiger une authentification forte par le payeur

On sait que l'une des innovations majeures de la directive (UE) 2015/2366 du Parlement européen et du Conseil (directive DSP 2) est d'avoir imposé aux prestataires de services de paiement d'exiger l'application d'un système d' authentification forte aux opérations présentant pour les payeurs les risques les plus élevés de fraude, et tout particulièrement les opérations de paiement à distance.

Comme l'expose le considérant 95 de la directive, « *La sécurité des paiements électroniques est fondamentale pour garantir la protection des utilisateurs et le développement d'un environnement sain pour le commerce électronique. Tous les services de paiement proposés par voie électronique devraient être sécurisés, grâce à des technologies permettant de garantir une authentification sûre de l'utilisateur et de réduire, dans toute la mesure du possible, les risques de fraude.* »

Transposant la directive, le code monétaire et financier prévoit en son article L. 133-44 que les prestataires de services de paiement doit appliquer l'authentification forte lorsque le payeur accède à son compte de paiement en ligne, initie une opération de paiement électronique ou exécute une opération par le biais d'un moyen de communication à distance, susceptible de comporter un risque de fraude.

L'article L. 133-19 V prévoit la sanction à appliquer en cas d'inobservance de cette obligation. Il précise 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 à l'article L. 133-44* ».

La chambre commerciale a été amenée à appliquer cette règle dans un arrêt publié du 30 août 2023 ayant fait l'objet de nombreux commentaires par la doctrine (Com., 30 août 2023, n° 22-11.707 , publié) :

Vu les articles L. 133-19, V, et L. 133-44 du code monétaire et financier dans leur rédaction issue de l'ordonnance n° 2017-1252 du 9 août 2017 :

4. Il ressort du premier de ces textes 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.

5. Il résulte de l'article 34, VIII, 3°, de l'ordonnance n° 2017-1252 du 9 août 2017, que le second, auquel renvoie le premier, 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.

6. Pour rejeter la demande de M. [F], le jugement retient qu'il a commis une négligence grave en faisant confiance à une personne qu'il ne connaissait pas et qui lui racontait une histoire assez peu crédible.

7. En se déterminant ainsi, sans rechercher, comme il lui incombait, si l'opération de paiement litigieuse avait été exécutée sans que la banque exige l'authentification forte du payeur, la cour d'appel n'a pas donné de base légale à sa décision.

Comme le relève un commentateur, *« La Haute Cour ne dit pas que le fait de communiquer son code ne constitue pas une négligence grave, mais qu'il faut avant tout examiner si les conditions d'examen sont réunies, c'est-à-dire si le système d'authentification forte avait été mis en place. Le tribunal de renvoi devra donc examiner si un tel système était ou non présent, avant d'éventuellement prendre en compte la négligence, ce qu'il ne saurait faire autrement. Ainsi, la solution apparaît stricte pour les établissements bancaires, mais compréhensible. La rigueur de la solution constitue une invitation faite aux établissements bancaires à la mise en place rapide d'un tel système, au risque de supporter invariablement les conséquences financières d'actes non autorisés, même en cas de négligence du client ».* [1]

Ce principe a été à nouveau affirmé par la chambre commerciale dans un arrêt du 22 octobre 2025 (Com. 22 octobre 2025, n° 24-19.749).

4.2. Analyse des griefs

4.2.1. Premier moyen

La société reproche à la cour d'appel d'avoir écarté la responsabilité de la banque en relevant l'existence de négligences graves du préposé du payeur alors qu'il résultait de ses propres constatations que l'opération n'avait pas été authentifiée grâce à la clé numérique prévue par la convention et qu'il incombe au prestataire de services, en application de l'article L. 133-23 du code monétaire et financier de prouver que l'opération a été authentifiée, dûment enregistrée et comptabilisée (premier grief)

La banque réplique en substance que l'opération a été effectuée sans le dispositif de sécurité personnalisé à la demande du payeur et conformément à une pratique établie et soutient que l'arrêt a bien établi en quoi cette opération effectuée après authentification par un fax signé du président de la société et confirmé par la seconde personne habilitée à émettre des ordres avait été authentifiée, dûment enregistrée et comptabilisée.

La société fait grief à l'arrêt d'avoir appliqué les dispositions de l'article L. 133-19 IV du code monétaire et financier relatives à la négligence grave du payeur alors que ce texte ne pouvait trouver application, la cour d'appel ayant constaté que l'ordre de paiement n'avait pas été transmis par un instrument de paiement doté de données de sécurité personnalisées (deuxième grief).

La banque réplique que c'est la société elle-même qui a demandé de ne pas appliquer le protocole d'authentification forte contractuellement prévu et d'accepter que les ordres de virements soient transmis par télécopie.

Dans une troisième branche, la société invoque un manque de base légale, la cour d'appel n'ayant pas recherché comme elle y était invitée, si la banque n'avait pas manqué à son

obligation d’exiger une authentification forte.

Selon la banque, la cour d’appel a procédé à cette recherche en retenant que l’envoi d’une télécopie signée par le président et confirmée par une autre personne habilitée à émettre des ordres de paiement constituait une authentification forte. Elle rappelle qu’en outre, c’est la société qui est a demandé à ne pas utiliser la clé prévue par la convention signée entre la banque et son client.

4.2.2. Second moyen

Il est reproché à la cour d’appel d’avoir retenu à l’encontre de la société une responsabilité délictuelle, en l’espèce celle du commettant du fait des fautes de ses préposés, alors que seul était applicable le régime de responsabilité défini par le code monétaire et financier, et d’avoir en outre violé le principe du non-cumul des responsabilités contractuelle et délictuelle, un contrat liant la banque et la société.

La banque réplique que la cour d’appel a seulement vérifié que les négligences graves alléguées étaient bien imputables à la société, la référence aux dispositions de l’article 1242 alinéa 5 du code civil relevant d’une maladresse de rédaction.

Il appartiendra à notre chambre de statuer sur les mérites de ces griefs à la lumière des principes rappelés plus haut.

---

1. D Mimoun, JCP E n° 48 du 30 novembre 2023, chronique droit bancaire.