**IDAI**

**DROIT BANCAIRE**

**Cours de J. LASSERRE CAPDEVILLE**

**TRAVAUX DIRIGÉS**

**Équipe pédagogique :**

**E. DERCOURT**

**Séance n° 4**

**Thème :** L’encadrement juridique des opérations de paiement par carte, virement et prélèvement

**Commentaire d’arrêt**

-Cass. com., 27 mars 2024, n° 22-21.200

**Fiches d’arrêts à préparer (penser à dégager une problématique)**

-Cass. com., 2 juillet 2025, n° 24-16.590

-Cass. com., 12 juin 2025, n° 24-13.777

-Cass. com., 30 août 2023, n° 22-11.707

**Commentaire d’arrêt**

**Cass. com., 27 mars 2024, n° 22-21.200**

Faits et procédure

1. Selon l'arrêt attaqué (Metz, 7 juillet 2022), entre novembre et décembre 2016, le compte ouvert dans les livres de la société Banque populaire Alsace Lorraine Champagne (la banque) au nom de la société Systran Software Inc. (la société) a été débité de diverses sommes en exécution de quatre ordres de virements transmis par courrier électronique, au profit de comptes situés à l'étranger.

2. Le 4 août 2017, soutenant qu'elle n'avait pas consenti à ces virements et que les ordres de virement ainsi que l'ordre de clôture d'un compte à terme, dont le versement du solde sur le compte courant de la société avait permis l'exécution d'un des ordres de virement, avaient été adressés par un tiers ayant piraté la messagerie électronique de M. [R], son dirigeant, la société a assigné la banque pour obtenir sa condamnation à lui restituer les sommes versées en exécution de ces ordres et à lui payer des dommages et intérêts.

Examen des moyens

(…)

Mais sur les premier et troisième moyens, réunis

Enoncé des moyens

4. Par son premier moyen, la banque fait grief à l'arrêt de la condamner à verser à la société la somme de 199 834,54 euros de dommages et intérêts au titre du préjudice causé par les quatre virements, alors « que la Cour de justice de l'Union européenne a dit pour droit que le régime de responsabilité des prestataires de service de paiement prévu par la directive 2007/64/CE était d'application exclusive dans les rapports entre le prestataire et l'utilisateur ; qu'il s'en évince que la responsabilité du prestataire de services de paiement à raison du manquement à l'une de ses obligations ne peut être recherchée que sur le fondement des articles L. 133-1 et suivants du code monétaire et financier, qui ont transposé cette directive en droit français ; que, pour condamner la banque à verser à la société la somme de 199 834,54 euros de dommages et intérêts au titre du préjudice causé par les quatre virements litigieux, la cour d'appel a jugé que sa responsabilité était engagée sur le fondement du droit commun pour manquement à son devoir de vigilance ; qu'en statuant ainsi, elle a violé l'article 1147, devenue 1231-1 du code civil, par fausse application. »

5. Par son troisième moyen, la banque fait grief à l'arrêt de la condamner à verser à la société la somme de 20 000 euros de dommages et intérêts au titre du préjudice lié à la clôture du compte à terme, alors « que la Cour de justice de l'Union européenne a dit pour droit que le régime de responsabilité des prestataires de service de paiement prévu par la directive 2007/64/CE était d'application exclusive dans les rapports entre le prestataire et l'utilisateur ; qu'il s'en évince que la responsabilité du prestataire de services de paiement à raison du manquement à l'une de ses obligations ne peut être recherchée que sur le fondement des articles L. 133-1 et suivants du code monétaire et financier, qui ont transposé cette directive en droit français ; que, pour condamner la banque à verser à la société la somme de 20 000 euros de dommages et intérêts au titre du préjudice lié à la clôture du compte à terme, avec intérêts au taux légal à compter du 15 décembre 2016, la cour d'appel a jugé que sa responsabilité était engagée sur le fondement du droit commun pour manquement à son devoir de vigilance ; qu'en statuant ainsi, elle a violé l'article 1147, devenue 1231-1, du code civil par fausse application.

Réponse de la Cour

(…)

Bien-fondé des moyens

Vu les articles 1231-1 du code civil, dans sa rédaction antérieure à celle issue de l'ordonnance n° 2017-1252 du 9 août 2017, L. 133-18 à L. 133-24 du code monétaire et financier :

9. La responsabilité contractuelle de droit commun prévue résultant du premier de ces textes n'est pas applicable en présence d'un régime de responsabilité exclusif.

10. Dans son arrêt du 16 mars 2023, Beobank (C-351/21), la Cour de justice a interprété en ces termes les article 58, 59 et 60 de la directive 2007/64/CE :

« 37 [...] le régime de responsabilité des prestataires de services de paiement prévu à l'article 60, paragraphe 1, de la directive 2007/64 ainsi qu'aux articles 58 et 59 de cette directive a fait l'objet d'une harmonisation totale. Cela a pour conséquence que sont incompatibles avec ladite directive tant un régime de responsabilité parallèle au titre d'un même fait générateur qu'un régime de responsabilité concurrent qui permettrait à l'utilisateur de services de paiement d'engager cette responsabilité sur le fondement d'autres faits générateurs (voir, en ce sens, arrêt du 2 septembre 2021, C-337/20, CRCAM, [...] points 42 et 46).

38 En effet, le régime harmonisé de responsabilité pour les opérations non autorisées ou mal exécutées établi dans la directive 2007/64 ne saurait être concurrencé par un régime alternatif de responsabilité prévu dans le droit national reposant sur les mêmes faits et le même fondement qu'à condition de ne pas porter préjudice au régime ainsi harmonisé et de ne pas porter atteinte aux objectifs et à l'effet utile de cette directive (arrêt du 2 septembre 2021, C-337/20, CRCAM, [...] point 45). »

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.

12. Pour condamner, sur le fondement de l'article 1231-1 du code civil, la banque à verser à la société certaines sommes en réparation des préjudices résultant de l'exécution des ordres de virement et de transfert litigieux, l'arrêt retient qu'il ressort des éléments de preuve sérieux et concordants que M. [R] n'était pas à l'origine des ordres qui ont été exécutés et qu'en les exécutant, tandis qu'ils présentaient des anomalies apparentes, la banque a manqué à son devoir contractuel de vigilance.

13. En statuant ainsi, alors que le titulaire des comptes contestait être l'auteur des ordres de transfert des fonds litigieux, ce dont il se déduisait que la responsabilité de la banque ne pouvait être recherchée que sur le fondement de l'article L. 133-18 du code monétaire et financier, la cour d'appel a violé les textes susvisés.

PAR CES MOTIFS, et sans qu'il y ait lieu de statuer sur les autres griefs, la Cour :

CASSE ET ANNULE, en toutes ses dispositions, l'arrêt rendu le 7 juillet 2022, entre les parties, par la cour d'appel de Metz ;

Remet l'affaire et les parties dans l'état où elles se trouvaient avant cet arrêt et les renvoie devant la cour d'appel de Nancy.

**Fiches d’arrêts à préparer (penser à dégager une problématique)**

**-Cass. com., 2 juillet 2025, n° 24-16.590**

Faits et procédure

1. Selon l'arrêt attaqué (Douai, 21 mars 2024), les 5 et 6 mars 2019, deux virements ont été effectués à partir du compte ouvert par M. [W] dans les livres de la caisse de Crédit mutuel de [Localité 3] (la banque).

2. Le 7 mars 2019, M. [W] a notifié à la banque qu'il contestait être à l'origine de ces deux opérations et lui en a demandé le remboursement.

3. La banque lui ayant opposé un refus, il l'a assignée en paiement le 21 décembre 2021.

Examen du moyen

Enoncé du moyen

4. M. [W] fait grief à l'arrêt attaqué de déclarer son action irrecevable, alors « qu'il résulte de l'article L. 133-24 du code monétaire et financier que l'utilisateur de services de paiement signale, sans tarder, à son prestataire de services de paiement une opération de paiement non autorisée ou mal exécutée et au plus tard dans les treize mois suivant la date de débit sous peine de forclusion à moins que le prestataire de services de paiement ne lui ait pas fourni ou n'ait pas mis à sa disposition les informations relatives à cette opération de paiement conformément au chapitre IV du titre 1er du livre III ; qu'en l'espèce, il est constant que le 7 mars 2019, il a formé opposition à deux opérations au débit de ses comptes bancaires réalisées dans la nuit du 5 au 6 mars 2019 pour des montants de 7 314,00 euros et 3 717,00 euros en déclarant ne pas en être à l'origine, et qu'il a ensuite, le 8 mars 2019, informé son agence bancaire de ces opérations frauduleuses, et lui a demandé le remboursement des sommes indûment prélevées ; qu'en le déclarant irrecevable aux motifs que l'article L. 133-24 du code monétaire et financier instaurait un délai de forclusion spécial de 13 mois, que les débits prétendument frauduleux remontaient au 6 mars 2019 et que l'assignation du 21 décembre 2021, soit largement plus de 13 mois plus tard, encourait donc la forclusion, quand ce texte prévoit seulement que le payeur doit "signale " cette opération dans le délai de treize mois suivant la date de débit sous peine de forclusion, ce qui, si le signalement a été réalisée dans ce délai, autorise le demandeur à engager une action en justice dans le délai de droit commun, la cour d'appel a méconnu le texte susvisé. »   
  
Réponse de la Cour

Vu l'article L. 133-24 du code monétaire et financier :

5. Aux termes de cet article, l'utilisateur de services de paiement signale, sans tarder, à son prestataire de services de paiement une opération de paiement non autorisée ou mal exécutée et au plus tard dans les treize mois suivant la date de débit sous peine de forclusion.

6. Pour déclarer irrecevables les demandes de M. [W], l'arrêt, après avoir constaté que celui-ci avait, le 7 mars 2019, formé opposition aux deux virements effectués à partir de son compte les 5 et 6 mars 2019 en déclarant ne pas en être à l'origine, retient que l'assignation en paiement ayant été délivrée le 21 décembre 2021, soit plus de treize mois plus tard, l'action encourt la forclusion.

7. En statuant ainsi, alors qu'il résultait de ses propres constatations que M. [W] avait signalé sans tarder et au plus tard dans le délai de treize mois les opérations non autorisées, ce qui l'autorisait à agir en paiement contre la banque dans le délai de droit commun, la cour d'appel a violé l'article susvisé.

PAR CES MOTIFS, la Cour :

CASSE ET ANNULE, en toutes ses dispositions, l'arrêt rendu le 21 mars 2024, entre les parties, par la cour d'appel de Douai ;

Remet l'affaire et les parties dans l'état où elles se trouvaient avant cet arrêt et les renvoie devant la cour d'appel de Douai autrement composée ;

**-Cass. com., 12 juin 2025, n° 24-13.777**

Faits et procédure

1. Selon l'arrêt attaqué (Paris, 7 février 2024), le 23 juillet 2019, Mme [W], salariée de la société [H] transport dirigée par M. [G] [H] (la société) a été contactée téléphoniquement par une personne se présentant comme un technicien de la société BNP Paribas (la banque) lui demandant d'effectuer différentes manipulations à l'aide du système de paiement à distance afin permettre la réinscription d'opérations sur le compte.

2. A la suite de ces manipulations, deux virements ont été exécutés vers des comptes domiciliés en Allemagne pour une somme totale de 98 000 euros.

3. Après avoir déposé une plainte pour escroquerie et soutenant ne pas avoir autorisé ces paiements, la société a assigné la banque en réparation de ses préjudices.

Examen du moyen

Enoncé du moyen

4. La banque fait grief à l'arrêt de la condamner à payer à la société la somme de 98 000 euros au titre du remboursement des fonds, alors :

« 1° que manque, par négligence grave, à son obligation de prendre toute mesure raisonnable pour préserver la sécurité de ses dispositifs de sécurité personnalisés, l'utilisateur d'un service de paiement qui communique les données personnelles de ce dispositif de sécurité en réponse à un appel téléphonique dont la teneur permet à un interlocuteur normalement attentif de douter de sa provenance ; qu'en l'espèce, la cour d'appel a relevé qu'il ressortait de l'audition de [G] [H] que " ([R] [W]) ne s'est pas méfiée de son interlocuteur qui ne lui demandait pas de mot de passe (...) ; qu'elle a renouvelé la création d'une signature électronique, son interlocuteur prétendant que la manoeuvre n'avait pas réussi " ; qu'elle a également relevé que l'audition de [R] [W] confirmait qu' " elle s'est connectée avec le boîtier et la carte, mais sans le mot de passe", que "l'escroc lui a alors demandé de se connecter et de se déconnecter à plusieurs reprises, puis de saisir la clef d'accès créée par le boîtier. Prétendant que cela ne fonctionnait pas, il lui a demandé d'essayer avec une autre clef d'accès qu'il lui a communiquée. Il lui a refait manipuler le boîtier à plusieurs reprises en l'embrouillant', puis lui a demandé de confirmer que le code qu'il lui indiquait au téléphone s'affichait, ce qui était le cas. Il lui a fait appuyer sur un ou deux boutons du boîtier, lui a demandé d'attendre et de confirmer. [R] [W] pense que c'est ce qui a créé une signature pour les virements" ; qu'en considérant qu' "il n'est pas démontré par la banque que la société [H] Transports ait commis une négligence grave exonérant la société BNP Paribas de son obligation de remboursement", quand il ressortait de ses propres constatations que Mme [W], et partant la société [H] Transports, avait communiqué les données personnelles de son dispositif de sécurité en réponse à un appel téléphonique dont la teneur permettait à un interlocuteur normalement attentif de douter de sa provenance, la cour d'appel a violé les articles L. 133-16 et L. 133-19 du code monétaire et financier ;

2°/ que les juges du fond ne peuvent statuer par voie de simple affirmation sans viser ni analyser, fût-ce sommairement, les éléments sur lesquels ils fondent leur décision ; qu'en première instance, le tribunal de commerce de Paris avait retenu " que Mme [W] a été contactée par téléphone (mais qu'[H] n'apporte pas la preuve qu'il s'agit du numéro de la hotline de BNP)" ; qu'en affirmant de manière péremptoire que " la circonstance que l'escroc ait pu usurper un numéro de téléphone de la société BNP Paribas (...) était de nature à persuader ([R] [W]) qu'elle était en relation avec un technicien de la banque", sans viser ni analyser, fût-ce sommairement, les éléments de preuve sur lesquels elle se fondait pour juger que l'appel provenait d'un numéro de téléphone attribué à la société BNP Paribas, la cour d'appel a violé l'article 455 du code de procédure civile ;

3°/ que commet une négligence grave l'utilisateur de services de paiement qui omet de prendre toute mesure nécessaire pour préserver la sécurité de ses dispositifs de sécurité personnalisés ; qu'en l'espèce, l'article III des conditions générales de fonctionnement de la Carte Transfert Sécurisé (CTS) stipule que le détenteur d'un code personnel communiqué confidentiellement par la société BNP Paribas doit "tenir son code confidentiel absolument secret et ne le communiquer à quiconque" ; que l'article VII précise que "le Détenteur est responsable de l'utilisation et de la conservation de la Carte et du code confidentiel qui y est associé et de leur utilisation conformément aux présentes conditions de fonctionnement", l'article VIII ajoutant que "le Client est tenu solidairement et indivisément responsable de toutes les conséquences financières résultant de l'utilisation et de la conservation de la Carte par son Détenteur" ; qu'il résultait, en outre du bordereau BNP Net Entreprises (production) que Mme [W], désignée comme mandataire "M3", n'était pas habilitée à valider les "virements domestiques/Sepa" et "virements internationaux " (" Choix des services et habilitation des mandataires") ; qu'en affirmant que "les documents contractuels et les guides et exemples d'utilisation du service BNP Net Evolution ne suffisent pas à établir les faits de négligence grave imputés à la société [H] Transports, consistant notamment à avoir laissé [R] [W] utiliser la Carte Transfert Sécurité de [G] [H]", sans expliquer comment cette dernière avait pu valider les virements litigieux quand seule la Carte Transfert Sécurisé (CTS) de [G] [H] permettait de valider les virements internationaux, la cour d'appel a privé son arrêt de base légale au regard des articles L. 133-16 et L. 133-19 du code monétaire et financier ;

4°/ que commet une négligence grave l'utilisateur de services de paiement qui omet de prendre toute mesure nécessaire pour préserver la sécurité de ses dispositifs de sécurité personnalisés ; qu'en l'espèce, la cour d'appel a relevé qu'il ressortait de l'audition de [G] [H] que "([R] [W]) ne s'est pas méfiée de son interlocuteur qui ne lui demandait pas de mot de passe (...) ; qu'elle a renouvelé la création d'une signature électronique, son interlocuteur prétendant que la manoeuvre n'avait pas réussi" ; qu'elle a également relevé que l'audition de [R] [W] confirmait qu'elle s'est connectée avec le boîtier et la carte, mais sans le mot de passe ", que l'escroc lui a alors demandé de se connecter et de se déconnecter à plusieurs reprises, puis de saisir la clef d'accès créée par le boîtier. Prétendant que cela ne fonctionnait pas, il lui a demandé d'essayer avec une autre clef d'accès qu'il lui a communiquée. Il lui a refait manipuler le boîtier à plusieurs reprises en l'embrouillant', puis lui a demandé de confirmer que le code qu'il lui indiquait au téléphone s'affichait, ce qui était le cas. Il lui a fait appuyer sur un ou deux boutons du boîtier, lui a demandé d'attendre et de confirmer. [R] [W] pense que c'est ce qui a créé une signature pour les virements " ; qu'il résultait de ces constatations que Mme [W] avait utilisé une CTS permettant de créer une signature pour la validation des virements internationaux, à savoir celle de [G] [H] ; qu'en affirmant, au contraire, qu' "il ne ressort pas de l'enquête de gendarmerie que [R] [W] ait utilisé la Carte Transfert Sécurisé de [G] [H] ", la cour d'appel qui n'a pas tiré les conséquences légales de ses propres constatations, a violé les articles L. 133-16 et L. 133-19 du code monétaire et financier. »

Réponse de la Cour

5. Après avoir exactement énoncé que, dans l'hypothèse d'ordres de paiement non autorisés, il appartient à la banque de fournir les éléments afin de prouver la faute ou la négligence grave commise par sa cliente, l'arrêt, se fondant sur les auditions par les services d'enquête du dirigeant et de l'employée de la société, retient que la secrétaire de cette société avait reçu un appel téléphonique d'un soi-disant employé de la banque l'avertissant d'une panne informatique qui avait fait disparaitre les écritures du matin, et qu'à la demande de l'escroc, cette employée, après s'être connectée au service de paiement en ligne à l'aide du dispositif de sécurité personnalisé mais sans le mot de passe, avait effectué diverses manipulations afin de reconstituer les écritures sans se méfier de son interlocuteur qui ne lui demandait pas de mot de passe. Il relève que la circonstance que l'escroc ait pu usurper un numéro de téléphone de la banque et annoncer le code qui s'affichait sur l'écran de l'utilisatrice était de nature à persuader celle-ci qu'elle était en relation avec un technicien. Il ajoute que la connaissance par son interlocuteur des opérations réalisées avant l'appel et de leur disparition pouvait la conforter dans la croyance qu'un incident informatique était survenu. Il retient encore que l'historique des opérations versé aux débats par la société révèle que le numéro d'abonné du titulaire de la carte de transfert sécurisé n'était pas attaché à la validation des tiers.

6. De ces constatations et appréciations, la cour d'appel a pu déduire que la société n'avait pas commis de négligence grave dans la conservation et l'utilisation de ses données personnelles de sécurité.

7. Le moyen n'est donc pas fondé.

PAR CES MOTIFS, la Cour :

REJETTE le pourvoi ;

**-Cass. com., 30 août 2023, n° 22-11.707**

Faits et procédure

1. Selon le jugement attaqué (Clermont-Ferrand, 13 janvier 2022), rendu en dernier ressort, soutenant qu'en réponse à un appel téléphonique et à un message, il avait communiqué à un tiers, qu'il pensait être un employé de la société Caisse régionale de crédit agricole mutuel Centre France (la banque), auprès de laquelle il avait ouvert un compte, le code à six chiffres, dénommé « 3D Secure », destiné à valider les paiements par internet à partir de ce compte et qu'à la suite de cette communication, un tel paiement, non réalisé par lui, avait été effectué le 27 janvier 2020, M. [X] a demandé à la banque de lui rembourser la somme qui avait été prélevée à ce titre et de réparer son préjudice.

2. Faisant valoir que M. [X] avait commis une négligence grave en communiquant volontairement un code de sécurité validant une opération financière à une personne extérieure, la banque s'est opposée à sa demande.

Moyens

Examen du moyen

Sur le premier moyen

Enoncé du moyen

3. M. [X] fait grief au jugement attaqué de rejeter l'intégralité de ses demandes, fins et conclusions, alors « 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 l'authentification forte prévue à l'article L. 133-44 du code monétaire et financier ; qu'en l'absence de respect de l'exigence d'authentification forte prévue à l'article L. 133-44 susmentionné, le prestataire de services de paiement ne peut donc opposer au payeur, pour refuser de l'indemniser d'une opération non autorisée, qu'il n'a pas satisfait intentionnellement ou par négligence grave aux obligations mentionnées aux articles L. 133-16 et L. 133-17 du code monétaire et financier ; qu'en déboutant M. [X] de sa demande de remboursement aux motifs qu'il avait commis une négligence grave, sans rechercher si, comme le soutenait le requérant, l'opération de paiement litigieuse du 27 janvier 2020 avait pu être exécutée sans que la banque ait exigé l'authentification forte prévue à l'article L. 133-44 susmentionné de sorte que la banque ne pouvait alors se prévaloir d'une négligence grave de son client, le tribunal a privé sa décision de base légale au regard de l'article L. 133-19 du code monétaire et financier, dans sa rédaction issue de l'ordonnance n° 2017-1252 du 9 août 2017, et de l'article L. 133-44 du code de monétaire et financier, dans sa rédaction issue de l'ordonnance n° 2017-1252 du 9 août 2017, entrée en vigueur le 14 septembre 2019, dix-huit mois après l'entrée en vigueur de l'acte délégué adopté en vertu de l'article 98.1 de la directive (UE) 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015. »

Motivation

Réponse de la Cour ;

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. [X], 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.

Dispositif

PAR CES MOTIFS, sans qu'il y ait lieu de statuer sur les autres griefs, la Cour :

CASSE ET ANNULE, en toutes ses dispositions, le jugement rendu le 13 janvier 2022, entre les parties, par le tribunal judiciaire de Clermont-Ferrand ;

Remet l'affaire et les parties dans l'état où elles se trouvaient avant ce jugement et les renvoie devant le tribunal judiciaire de Clermont-Ferrand, autrement composé ;