COMM.

FB

COUR DE CASSATION

_____

Audience publique du 24 novembre 2021

Cassation

M. GUÉRIN, conseiller doyen
faisant fonction de président

Arrêt n° 811 F-D

Pourvoi n° C 20-13.767

R É P U B L I Q U E F R A N Ç A I S E

_____

AU NOM DU PEUPLE FRANÇAIS

_____

ARRÊT DE LA COUR DE CASSATION, CHAMBRE COMMERCIALE, FINANCIÈRE ET ÉCONOMIQUE, DU 24 NOVEMBRE 2021

La société Caisse de crédit mutuel de [Localité 4], société coopérative de crédit, dont le siège est [Adresse 2], a formé le pourvoi n° C 20-13.767 contre le jugement rendu le 17 décembre 2019 par le tribunal d'instance de Lens, dans le litige l'opposant à M. [C] [W], domicilié [Adresse 3], défendeur à la cassation.

La demanderesse invoque, à l'appui de son pourvoi, le moyen unique de cassation annexé au présent arrêt.

Le dossier a été communiqué au procureur général.

Sur le rapport de Mme Fèvre, conseiller, les observations de la SCP Célice, Texidor, Périer, avocat de la société Caisse de crédit mutuel de [Localité 4], de la SCP Boré, Salve de Bruneton et Mégret, avocat de M. [W], et l'avis de Mme Guinamant, avocat général référendaire, après débats en l'audience publique du 5 octobre 2021 où étaient présents M. Guérin, conseiller doyen faisant fonction de président, Mme Fèvre, conseiller rapporteur, M. Ponsot, conseiller, et Mme Mamou,

greffier de chambre,

la chambre commerciale, financière et économique de la Cour de cassation, composée des président et conseillers précités, après en avoir délibéré conformément à la loi, a rendu le présent arrêt.

Faits et procédure

1. Selon le jugement attaqué (tribunal d'instance de Lens, 17 décembre 2019), rendu en dernier ressort, M. [W], titulaire d'un compte dans les livres de la société Caisse de crédit mutuel de [Localité 4] (la banque) a contesté trois opérations de paiement effectuées frauduleusement sur ce compte à la suite de sa réponse à un courriel, reçu le 27 décembre 2017, l'ayant conduit à communiquer sur le site internet proposé le numéro de sa carte bancaire avec sa date d'expiration, le code de vérification, et lui en a demandé le remboursement.

2. La banque lui ayant opposé un refus, estimant qu'il avait commis une négligence grave en communiquant ses données personnelles en réponse à un courriel suspect, M. [W] l'a assignée en paiement.

Sur le moyen, pris en sa première branche

Enoncé du moyen

3. La banque fait grief au jugement de la condamner à payer à M. [W] la somme de 2 593 euros, assortie des intérêts au taux légal à compter du 8 novembre 2018, date de la mise en demeure, et de rejeter ses demandes, alors « 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 courriel qui contient des indices permettant à un utilisateur normalement averti de douter de sa provenance, peu important qu'il soit, ou non, avisé des risques d'hameçonnage ; qu'en l'espèce, la banque faisait valoir que le courriel du 27 décembre 2017, produit aux débats par M. [W], auquel ce dernier avait admis avoir répondu en communiquant son numéro de carte bancaire, le pictogramme et son numéro de téléphone, comportait des indices qui permettaient à un utilisateur normalement averti de douter de sa provenance, dans la mesure où l'adresse de l'expéditeur de ce courriel était "[Courriel 1] (illisible)[Courriel 1]", que son objet était intitulé "***SPAM*** vous écrit", et que le message de ce courriel, qui indiquait "lors de votre dernier achat, vous été [sic] averti par un message vous informant de l'obligation d'adhérer à la nouvelle réglementation concernant la fiabilité des achats par CB sur internet et la mise en place d'un arrêt pour vos futurs achats. Or, nous n'avons pas à ce jour d'adhésion de votre part et nous sommes au regret de vous informer que vous pouvez plus [sic] utiliser votre carte sur internet", en invitant le destinataire à cliquer sur un lien avec de communiquer ses données personnelles, comportait des fautes de syntaxe et d'orthographe, et ne correspondait pas à la situation de M. [W] qui ne pouvait ignorer que lors de son dernier achat sur internet, il n'avait reçu aucun avertissement quant à un risque de blocage de sa carte pour effectuer des paiements à distance ; que, pour néanmoins faire droit à la demande de M. [W] de remboursement des opérations de paiement réalisées sur son compte le lendemain de sa réponse à ce courriel frauduleux, le tribunal d'instance, après avoir constaté que M. [W] avait admis avoir fourni ses identifiants en réponse à ce courriel, a retenu que la banque "ne rapporte pas la preuve de ce que M. [W] a fourni en pleine connaissance de cause ces éléments et que celui-ci aurait encore failli à son devoir de vigilance, en n'ayant pas vérifié l'origine de l'email litigieux ou qu'il ait manqué à ses obligations contractuelles", que M. [W] avait immédiatement fait opposition dès qu'il avait été informé des débits frauduleux effectués sur son compte, que la banque ne démontrait pas avoir alerté M. [W] sur les risques d'hameçonnage, et enfin, que le client de la banque avait raisonnablement pu s'inquiéter d'un message l'informant que s'il ne procédait pas à cette demande d'adhésion en ligne, rapidement, il perdrait alors l'usage de sa carte bancaire sur internet ; qu'en statuant de la sorte, sans rechercher, ainsi qu'elle y était invitée, si le courriel d'hameçonnage auquel M. [W] avait reconnu avoir répondu en communiquant les données confidentielles de sa carte bancaire ne comportait pas des indices permettant à un utilisateur normalement averti de douter de sa provenance, de sorte qu'en y répondant, M. [W] avait commis une négligence grave exonérant la banque de son obligation de remboursement, le tribunal d'instance a privé sa décision de base légale au regard des articles L. 133-16 et L. 133-19 du code monétaire et financier dans leur version applicable en la

cause. »

Réponse de la Cour

Vu les articles L. 133-16 et L. 133-19 du code monétaire et financier dans leur rédaction antérieure à celle issue de l'ordonnance n° 2017-1252 du 9 août 2017 :

4. Il résulte du premier de ces textes que l'utilisateur de services de paiement prend toute mesure raisonnable pour préserver la sécurité de ses dispositifs de sécurité personnalisés et du second que le payeur supporte toutes les pertes occasionnées par des opérations de paiement non autorisées si 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.

5. Pour condamner la banque à payer à M. [W] la somme de 2 593 euros en remboursement des paiements non autorisés effectués sur son compte, le jugement retient que, s'il est établi que ce dernier a fourni ses identifiants permettant l'accès à son compte en ligne après avoir reçu un courriel frauduleux, la banque ne démontre pas qu'il a fourni ces informations en pleine connaissance de cause et qu'il aurait failli à son devoir de vigilance dès lors qu'il n'avait pas à vérifier l'origine du message et qu'il a pu raisonnablement s'inquiéter à la réception d'un courriel l'informant que, s'il ne procédait pas rapidement à l'adhésion en ligne, il perdrait l'usage de sa carte bancaire sur internet.

6. En se déterminant ainsi, sans rechercher, au regard des circonstances de l'espèce, si M. [W] n'aurait pas pu avoir conscience que le courriel qu'il avait reçu le 27 décembre 2017 était frauduleux et si, en conséquence, le fait d'avoir communiqué ses données personnelles ne caractérisait pas un manquement par négligence grave à ses obligations mentionnées à l'article L. 133-16 du code monétaire et financier, le tribunal d'instance n'a pas donné de base légale à sa décision.

PAR CES MOTIFS, et sans qu'il y ait lieu de statuer sur l'autre grief, la Cour :

CASSE ET ANNULE, en toutes ses dispositions, le jugement rendu le 17 décembre 2019, entre les parties, par le tribunal d'instance de Lens ;

Remet l'affaire et les parties dans l'état où elles se trouvaient avant ce jugement et les renvoie devant le tribunal de proximité d'Arras ;

Condamne M. [W] aux dépens ;

En application de l'article 700 du code de procédure civile, rejette les demandes formées par M. [W] et la société Caisse de crédit mutuel de [Localité 4] ;

Dit que sur les diligences du procureur général près la Cour de cassation, le présent arrêt sera transmis pour être transcrit en marge ou à la suite du jugement cassé ;

Ainsi fait et jugé par la Cour de cassation, chambre commerciale, financière et économique, et prononcé par le président en son audience publique du vingt-quatre novembre deux mille vingt et un.

MOYEN ANNEXE au présent arrêt

Moyen produit par la SCP Célice, Texidor, Périer, avocat aux Conseils, pour la société Caisse de crédit mutuel de [Localité 4].

Il est fait grief au jugement attaqué D'AVOIR condamné la Caisse de Crédit Mutuel de [Localité 4] à payer à Monsieur [C] [W] la somme de 2.593 €, assortie des intérêts au taux légal à compter du 8 novembre 2018, date de la mise en demeure,

et D'AVOIR débouté la Caisse de Crédit Mutuel de [Localité 4] de ses demandes ;

AUX MOTIFS QUE « Sur la demande principale : Aux termes de l'article L. 133-18 du Code monétaire et financier, « En cas d'opération de paiement non autorisée signalée par l'utilisateur dans les conditions prévues à l'article L. 133-24, le prestataire de services de paiement du payeur rembourse immédiatement au payeur le montant de l'opération non autorisée et, le cas échéant, rétablir le compte débité dans l'état où il se serait trouvé si l'opération de paiement non autorisée n'avait pas eu lieu. Le payeur et son prestataire de services de paiement peuvent décider contractuellement d'une indemnité complémentaire ». L'article L. 133-19 du même code ajoute que : « I. – En cas d'opération de paiement non autorisée consécutive à la perte ou au vol de l'instrument de paiement, le payeur supporte, avant l'information prévue à l'article L. 133-17, les pertes liées à l'utilisation de cet instrument, dans la limite d'un plafond de 150 euros. Toutefois, la responsabilité du payeur n'est pas engagée en cas d'opération de paiement non autorisée effectuée sans utilisation du dispositif de sécurité personnalisé. II. La responsabilité du payeur n'est pas engagée si l'opération de paiement non autorisée a été effectuée en détournant, à l'insu du payeur, l'instrument de paiement ou les données qui lui sont liées. Elle n'est pas engagée non plus en cas de contrefaçon de l'instrument de paiement si, au moment de l'opération de paiement non autorisée, le payeur était en possession de son instrument. III. - Sauf agissement frauduleux de sa part, le payeur ne supporte aucune conséquence financière si le prestataire de services de paiement ne fournit pas de moyens appropriés permettant l'information aux fins de blocage de l'instrument de paiement prévue à l'article L. 133-17. IV. - Le payeur supporte toutes les pertes occasionnées par des opérations de paiement non autorisées si 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 ». Au sens des textes précités, le titulaire de la carte supporte la perte subie s'il lui est imputable une négligence d'une extrême gravité confinant au dol et dénotant une inaptitude de sa part à l'accomplissement de ses obligations contractuelles, et il est de principe qu'il appartient à l'émetteur de la carte, qui se prévaut d'une telle faute d'en rapporter la preuve, la circonstance que la carte ait été utilisée par un tiers avec l'utilisation d'identifiants confidentiels étant, -à elle seule, insusceptible de constituer cette preuve. Il appartient donc à la banque de rapporter la preuve que seule la négligence grave de son client peut être à l'origine des paiements frauduleux. En l'espèce, il est constant que, le 28 décembre 2017, Monsieur [C] [W] a été averti par l'envoi d'un SMS de l'utilisation de sa carte bancaire pour trois opérations de paiement en ligne intervenues la veille en début de soirée auprès de la société Cdiscount et qu'il a formé opposition à l'usage de ladite carte le jour-même et a effectué un dépôt de plainte auprès du commissariat de Noeux-les-Mines. Pour s'opposer à sa demande de remboursement du montant des opérations réalisées avec cette carte avant l'opposition, la CAISSE DE CREDIT MUTUEL de [Localité 4] évoque la faute de son client en application des dispositions de l'article L. 133-19 du Code Monétaire et Financier aux termes duquel le payeur supporte toutes les pertes occasionnées par des opérations de paiement non autorisées s'il n'a pas satisfait intentionnellement ou par négligence grave aux obligations mentionnées aux articles L133-16 et L133-17 de prendre toute mesure pour préserver la sécurité de ses dispositifs de sécurité personnalisés et de faire opposition sans tarder en cas de vol. Il n'est pas contesté qu'en l'espèce, les opérations litigieuses d'achat n'ont pu être réalisées par leur auteur qu'en ayant connaissance des éléments d'identification confidentiels du client de la banque : identifiant et mot de passe pour l'accès au site de la banque en ligne, code confidentiel parmi les 64 codes délivrés sur une carte de clefs personnelles donnée par la banque à son client. Monsieur [C] [W] ne conteste d'ailleurs pas avoir répondu à un email, qui s'est avéré par la suite frauduleux, arguant cependant du fait qu'il a été induit en erreur et donc trompé, dans la mesure où le mail reçu comportait le logo du Crédit Mutuel, ainsi que toutes les caractéristiques pouvant être retrouvées sur les mails couramment adressés par la banque à ses clients. Il en résulte que Monsieur [W] admet avoir fourni ses identifiants permettant l'accès à son compte en ligne, après avoir reçu un courriel frauduleux. Cependant, de son côté, la banque ne rapporte pas la preuve de ce que Monsieur [C] [W] a fourni en pleine connaissance de cause ces éléments et que celui-ci aurait encore failli à son devoir de vigilance, en n'ayant pas vérifié l'origine de l'email litigieux ou qu'il ait manqué à ses obligations contractuelles. Sachant que dès que Monsieur [C] [W] a eu connaissance de ces opérations frauduleuses, soit le lendemain matin des achats opérés en début de soirée du 27 décembre 2017, il a régularisé opposition de sa carte bancaire auprès de sa banque et a déposé plainte auprès du commissariat de son domicile. Le CREDIT MUTUEL de [Localité 4] se prévaut également d'un message d'alerte sur les risques de phishing publié au début de l'année 2015, aux termes duquel la banque aurait rappelé à ses sociétaires qu'ils ne devaient en aucune façon répondre à ce type d'email, soulignant encore que ce message d'alerte apparaitrait à chaque connexion tant que l'utilisateur n'aurait pas cliqué sur l'onglet "j'ai lu". Toutefois, outre le fait que la banque ne produit pas aux débats une copie de ce message d'alerte, il n'est pas non plus justifié que cette alerte a bien été adressée à Monsieur [C] [W] en 2015 et, encore moins que ce dernier y avait encore accès en 2017, alors même que cette information est antérieure à la

fraude dont il a été victime. La banque ne démontre pas non plus que Monsieur [W] avait encore accès à ce message d'alerte le 27 décembre 2017, jour des opérations frauduleuses. De même, les procès-verbaux de constat produits aux débats par le CREDIT MUTUEL de [Localité 4], consistant en la capture d'écran de son site, comprenant notamment des informations relatives à la sécurité sur Internet, datent du 8/12/2014 et 10/02/2015, ne sont pas probants en ce qu'ils sont antérieurs à la fraude dont a été victime Monsieur [W] et ne permettent pas d'attester de ce qu'ils étaient toujours d'actualité au mois de décembre 2017. En outre, le fait que Monsieur [W] puisse réaliser de manière habituelle des achats en ligne depuis 2009, n'est pas un élément suffisant pour lui opposer une négligence grave ; étant même remarqué qu'étant coutumier d'achats en ligne, le demandeur a pu raisonnablement s'inquiéter de la réception de ce courriel l'informant que s'il ne procédait pas à cette demande d'adhésion en ligne, rapidement, il perdrait alors l'usage de sa carte bancaire sur internet. Aussi, le CREDIT MUTUEL de [Localité 4] ne rapporte pas la preuve de ce que Monsieur [C] [W] aurait manqué à son obligation de prendre toute mesure raisonnable pote préserver la sécurité de ses dispositifs de sécurité personnalisé, ou encore qu'il aurait nécessairement communiqué ses informations personnelles et confidentielles à un tiers par négligence grave ou par manquement intentionnel aux obligations lui incombant en la matière, voir même qu'il aurait agi frauduleusement. En conséquence, il convient de condamner la CAISSE de CREDIT MUTUEL de [Localité 4] à rembourser à Monsieur [C] [W] les sommes indûment prélevées sur son compte bancaire, à savoir la somme de 2.593 euros, assortie des intérêts au taux légal à compter du 8 novembre 2018, date de la mise en demeure. Sur les demandes accessoires. En vertu de l'article 696 du Code de Procédure Civile, la partie perdante est condamnée aux dépens. La CAISSE DE CREDIT MUTUEL de [Localité 4] sera donc condamnée aux dépens. En application des dispositions de l'article 700 du Code de Procédure Civile, le juge condamne la partie tenue aux dépens ou, à défaut, la partie perdante, à payer à l'autre partie la somme qu'il détermine au titre des frais exposés et non compris dans les dépens. En l'espèce, la CAISSE DE CREDIT MUTUEL de [Localité 4] sera condamnée au paiement de la somme de 500 euros au titre de l'article 700 du Code de procédure civile »

1°) ALORS 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 courriel qui contient des indices permettant à un utilisateur normalement averti de douter de sa provenance, peu important qu'il soit, ou non, avisé des risques d'hameçonnage ; qu'en l'espèce, la Caisse de Crédit Mutuel de [Localité 4] faisait valoir (ses conclusions reprises oralement à l'audience, p. 3 à 5) que le courriel du 27 décembre 2017, produit aux débats par Monsieur [W] (sa pièce n°1), auquel ce dernier avait admis avoir répondu en communiquant son numéro de carte bancaire, le pictogramme et son numéro de téléphone, comportait des indices qui permettaient à un utilisateur normalement averti de douter de sa provenance, dans la mesure où l'adresse de l'expéditeur de ce courriel était « [Courriel 1] (illisible)[Courriel 1] », que son objet était intitulé : « ***SPAM***vous écrit », et que le message de ce courriel, qui indiquait « lors de votre dernier achat, vous été [sic] averti par un message vous informant de l'obligation d'adhérer à la nouvelle réglementation concernant la fiabilité des achats par CB sur internet et la mise en place d'un arrêt pour vos futurs achats. Or, nous n'avons pas à ce jour d'adhésion de votre part et nous sommes au regret de vous informer que vous pouvez plus [sic] utiliser votre carte sur internet », en invitant le destinataire à cliquer sur un lien avec de communiquer ses données personnelles, comportait des fautes de syntaxe et d'orthographe, et ne correspondait pas à la situation de Monsieur [W] qui ne pouvait ignorer que lors de son dernier achat sur internet, il n'avait reçu aucun avertissement quant à un risque de blocage de sa carte pour effectuer des paiements à distance ; que, pour néanmoins faire droit à la demande de Monsieur [W] de remboursement des opérations de paiement réalisées sur son compte le lendemain de sa réponse à ce courriel frauduleux, le tribunal d'instance, après avoir constaté que Monsieur [W] avait admis avoir fourni ses identifiants en réponse à ce courriel, a retenu que la banque « ne rapporte pas la preuve de ce que Monsieur [C] [W] a fourni en pleine connaissance de cause ces éléments et que celui-ci aurait encore failli à son devoir de vigilance, en n'ayant pas vérifié l'origine de l'email litigieux ou qu'il ait manqué à ses obligations contractuelles », que Monsieur [W] avait immédiatement fait opposition dès qu'il avait été informé des débits frauduleux effectués sur son compte, que la banque ne démontrait pas avoir alerté Monsieur [W] sur les risques d'hameçonnage, et enfin, que le client de la banque avait raisonnablement pu s'inquiéter d'un message l'informant que s'il ne procédait pas à cette demande d'adhésion en ligne, rapidement, il perdrait alors l'usage de sa carte bancaire sur internet ; qu'en statuant de la sorte, sans rechercher, ainsi qu'elle y était invitée, si le courriel d'hameçonnage auquel Monsieur [W] avait reconnu avoir répondu en communiquant les données confidentielles de sa carte bancaire ne comportait pas des indices permettant à un utilisateur normalement averti de douter de sa provenance, de sorte qu'en y répondant, Monsieur [W] avait commis une négligence grave exonérant la banque de son obligation de remboursement, le tribunal d'instance a privé sa décision de base légale au regard des

articles L. 133-16 et L. 133-19 du code monétaire et financier (dans leur version applicable en la cause) ;

2°) ALORS, EN OUTRE, QUE les juges du fond doivent examiner, fût-ce de manière sommaire, les éléments de preuve soumis à leur examen ; qu'en se bornant à retenir, pour statuer comme il l'a fait, que si Monsieur [W] admettait avoir fourni ses identifiants permettant l'accès à son compte en ligne, après avoir reçu un courriel frauduleux, la banque « ne rapporte pas la preuve de ce que Monsieur [C] [W] a fourni en pleine connaissance de cause ces éléments et que celui-ci aurait encore failli à son devoir de vigilance, en n'ayant pas vérifié l'origine de l'email litigieux ou qu'il ait manqué à ses obligations contractuelles », et que Monsieur [W] avait pu raisonnablement s'inquiéter d'un message l'informant que s'il ne procédait pas à cette demande d'adhésion en ligne, rapidement, il perdrait alors l'usage de sa carte bancaire sur internet, sans procéder à l'examen du courriel d'hameçonnage en cause, le tribunal d'instance a violé l'article 455 du code de procédure civile.