6 juin 2018
Cour de cassation
Pourvoi nº 16-29.065

Chambre commerciale financière et économique - Formation restreinte hors RNSM/NA

ECLI:FR:CCASS:2018:CO00502

Texte de la **décision**

Entête

COMM.

FB

COUR DE CASSATION

_____

Audience publique du 6 juin 2018

Cassation partielle

M.RÉMERY, conseiller doyen
faisant fonction de président

Arrêt n° 502 F-D

Pourvoi n° Y 16-29.065

R É P U B L I Q U E F R A N Ç A I S E

_____

AU NOM DU PEUPLE FRANÇAIS

_____

LA COUR DE CASSATION, CHAMBRE COMMERCIALE, FINANCIÈRE ET ÉCONOMIQUE, a rendu l'arrêt suivant :

Statuant sur le pourvoi formé par :

1°/ la Caisse de crédit mutuel de Fruges, société coopérative de crédit, dont le siège est [...] ,

2°/ la Caisse fédérale du crédit mutuel Nord Europe, société coopérative à forme anonyme à capital variable, dont le siège est [...] ,

contre l'arrêt rendu le 3 novembre 2016 par la cour d'appel de Douai (chambre 8, section 1), dans le litige les opposant à Mme Huguette Y..., domiciliée [...] ,

défenderesse à la cassation ;

Les demanderesses invoquent, à l'appui de leur pourvoi, le moyen unique de cassation annexé au présent arrêt ;

Vu la communication faite au procureur général ;

LA COUR, en l'audience publique du 10 avril 2018, où étaient présents : M. Rémery, conseiller doyen faisant fonction de président, M.Remeniéras, conseiller rapporteur, M. Guérin, conseiller, M. Graveline, greffier de chambre ;

Sur le rapport de M.Remeniéras, conseiller, les observations de la SCP Célice, Soltner, Texidor et Périer, avocat de la Caisse de crédit mutuel de Fruges et de la Caisse fédérale du crédit mutuel Nord Europe, de la SCP Ohl et Vexliard, avocat de Mme Y..., l'avis de M. Le Mesle, premier avocat général, et après en avoir délibéré conformément à la loi ;

Donne acte à la Caisse fédérale du crédit mutuel Nord Europe du désistement de son pourvoi ;

Moyens

Sur le moyen unique, pris en ses deuxième et troisième branches :

Motivation

Vu les articles L. 133-16 et L. 133-19 du code monétaire et financier ;

Attendu 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 ces dispositifs de sécurité en réponse à un courriel qui contient des indices permettant à un utilisateur normalement attentif de douter de sa provenance ;

Exposé du litige

Attendu, selon l'arrêt attaqué, que Mme Y..., titulaire d'un compte dans les livres de la Caisse de crédit mutuel de Fruges (la Caisse), a contesté des opérations de paiement effectuées, selon elle, frauduleusement sur ce compte au moyen de sa carte bancaire et demandé à la Caisse de lui en rembourser le montant ; que se heurtant au refus de celle-ci, qui lui reprochait d'avoir commis une faute en communiquant à des tiers des informations confidentielles permettant d'effectuer les opérations contestées, Mme Y... l'a assignée en paiement ;

Attendu que pour condamner la Caisse à rembourser à Mme Y... les sommes prélevées sur son compte, l'arrêt retient que si celle-ci avait communiqué des données confidentielles ayant rendu possibles les prélèvements contestés en répondant à un courriel comportant le logotype de son opérateur de téléphonie, l'utilisatrice de service de paiement n'avait cependant pas commis de négligence grave, dès lors que ce courriel, dépourvu d'anomalies grossières et revêtant l'apparence générale de l'authenticité, avait surpris sa vigilance ;

Motivation

Qu'en statuant ainsi, après avoir relevé que Mme Y... réglait ses factures de téléphone par prélèvements et non par carte bancaires et qu'un examen attentif du courriel de rappel de paiement révélait de sérieuses irrégularités, de nature à faire douter de sa provenance, telles que l'inexactitude de l'adresse de l'expéditeur et du numéro du contrat mentionné ainsi que la discordance entre les montants réclamés, la cour d'appel, qui n'a pas tiré les conséquences légales de ses constatations, a violé les textes susvisés ;

Dispositif

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

CASSE ET ANNULE, sauf en ce que, confirmant de ce chef le jugement déféré, il déclare irrecevables les demandes de Mme Y... dirigées contre la Caisse fédérale de crédit mutuel Nord Europe, l'arrêt rendu le 3 novembre 2016, entre les parties, par la cour d'appel de Douai ; remet, en conséquence, sur les autres points, la cause et les parties dans l'état où elles se trouvaient avant ledit arrêt et, pour être fait droit, les renvoie devant la cour d'appel d'Amiens ;

Condamne Mme Y... aux dépens ;

Vu l'article 700 du code de procédure civile, rejette les demandes ;

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 de l'arrêt partiellement 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 six juin deux mille dix-huit.

Moyens annexés

MOYEN ANNEXE au présent arrêt

Moyen produit par la SCP Célice, Soltner, Texidor et Périer, avocat aux Conseils, pour la Caisse de crédit mutuel de Fruges.

Il est fait grief à l'arrêt infirmatif attaqué D'AVOIR condamné la Caisse de Crédit Mutuel de FRUGES à rembourser à Madame Huguette Y... les sommes de 6 432,93 euros au titre des opérations de paiement non autorisées et 25,90 euros au titre des frais bancaires, D'AVOIR condamné la Caisse de Crédit Mutuel de FRUGES à payer à Madame Huguette Y... la somme de 1 000 euros à titre de dommages et intérêts, D'AVOIR condamné la Caisse de Crédit Mutuel de FRUGES à payer à Madame Huguette Y... la somme de 1 500 euros par application de l'article 700 du code de procédure civile, et D'AVOIR condamné la Caisse de Crédit Mutuel de FRUGES aux dépens de première instance et d'appel,

AUX MOTIFS QUE « sur le fond, que selon le paragraphe I de l'article L. 133-19 du code monétaire et financier, dans sa rédaction issue de l'ordonnance n° 2009-866 du juillet 2009 applicable en l'espèce, 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 ; que 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 ; Que selon son paragraphe 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 ; qu'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 ; Que le paragraphe IV de ce même article prévoit toutefois 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 ; Que l'article L. 133-16 du code monétaire et financier prévoit précisément 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 dispositifs de sécurité personnalisés ; qu'il utilise l'instrument de paiement conformément aux conditions régissant sa délivrance et son utilisation ; Que l'article L. 133-17 du même code dispose pour sa part que lorsqu'il a connaissance de la perte, du vol, du détournement ou de toute utilisation non autorisée de son instrument de paiement ou des données qui lui sont liées, l'utilisateur de services de paiement en informe sans tarder, aux fins de blocage de l'instrument, son prestataire ou l'entité désignée par celui-ci ; Qu'en application de l'article L. 133-18, 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, rétablit 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 pouvant décider contractuellement d'une indemnité complémentaire ; Que l'article L.133-20 prévoit enfin qu'après avoir informé son prestataire ou l'entité désignée par celui-ci, conformément à l'article L. 133-17 aux fins de blocage de l'instrument de paiement, le payeur ne supporte aucune conséquence financière résultant de l'utilisation de cet instrument de paiement ou de l'utilisation détournée des données qui lui sont liées, sauf agissement frauduleux de sa part ; Que ces dispositions posent ainsi le principe de la prise en charge par la banque de toute utilisation frauduleuse d'un instrument de paiement mis à disposition du client, comme en l'espèce, une carte bancaire, qui serait la conséquence d'une défaillance technique du dispositif de sécurité ou qui ne serait pas imputable à une démarche frauduleuse ou une négligence grave du client ; Qu'il ressort des éléments du dossier et notamment de l'examen du relevé bancaire de l'appelante et du rapport de faits dressé le 28 août 2014 par le service de fonction monétique de la Caisse de Crédit Mutuel de Fruges que le compte de Madame Y... a été débité le 28 juillet 2016 d'une somme totale de 6 432,93 euros correspondant à sept opérations d'achat d'un montant de 918,99 euros chacune, effectuées le 25 juillet 2016 entre 21 heures heures 10, soit en l'espace d'à peine plus d'une heure à partir de la carte bancaire Mastercard Gold de Madame Y... sur le site marchand Free Mobile ; Qu'il n'est pas contesté que ce site utilise le protocole sécurisé de paiement sur Internet 3D Secure qui permet aux marchands de limiter les risques de fraude sur Internet, liés au tentatives d'usurpation d'identité et qui consiste à s'assurer, lors de chaque paiement en ligne, que la carte de paiement utilisée l'est par son véritable propriétaire ; que s'agissant du Crédit Mutuel, en plus des informations usuelles fournies pour tout paiement (numéro de carte bancaire, date d'expiration de la carte et les trois chiffres du code de sécurité imprimés au dos de la carte), l'internaute doit saisir un code à usage unique reçu par SMS ou via un serveur vocal interactif sur le numéro de téléphone associé à son compte bancaire ; Qu'avisée de la contestation de Madame Y... qui nie être l'auteur des opérations de paiements effectuées le 25 juillet 2016 à partir de sa carte bancaire, la Caisse de Crédit Mutuel de Fruges justifie avoir, ainsi que les dispositions de l'article L. 133-23 du code monétaire et financier le lui

imposaient, fait diligences pour effectuer des recherches et rassembler tous éléments suffisants de nature à établir le caractère non autorisé par le porteur, des opérations effectuées à l'aide des données des cartes de paiement virtuelles ; Ainsi que le rapport du service Fonction Monétique de la banque a permis d'établir que les opérations d'achat ont été réalisées à partir de deux adresses IP distinctes et que les codes à usage unique ayant servi à valider chacun des sept achats litigieux après communication des données attachées à la carte bancaire de Madame Y... ont été adressés via le serveur vocal interactif de la banque sur un numéro de téléphone fixe dont il n'est pas contesté qu'il s'agit de celui de Madame Y... ; Que si la Caisse de Crédit Mutuel de Fruges rapporte ainsi la preuve, conformément à l'article L. 133-23 précité du code monétaire et financier, que les opérations de paiements contestées ont été authentifiées, dûment enregistrées et comptabilisées, il n'en demeure pas moins que les utilisations successives des données attachées à la carte bancaire de Madame Y... telles qu'enregistrées par la banque ne suffisent pas nécessairement en tant que telles à prouver que les opérations ont été autorisées par elle ou que celle-ci n'a pas satisfait intentionnellement ou par négligence grave aux obligations lui incombant en la matière ; Que pour imputer à Madame Y... la totalité des paiements réalisés le 25 juillet 2014 à partir de sa carte bancaire, la Caisse de Crédit Mutuel de Fruges fait valoir que le détournement des données attachées à cette carte et au compte de téléphonie ouvert au nom de sa cliente auprès de SFR, n'a pas eu lieu à l'insu de Madame Y... et qu'en répondant au message du 25 juillet 2014 qui ne provenait manifestement pas de la société SFR et en communiquant ainsi volontairement l'ensemble de ses données bancaires personnelles composant le protocole sécurisé de paiement par carte bancaire mais également les informations relatives à son compte chez SFR, Madame Y... a commis une imprudence dans la conservation de celles-ci, constitutive d'une négligence grave au sens de l'article L. 133-19 précité du code monétaire et financier, qui la prive de la protection offerte par la loi au payeur, titulaire de la carte ; qu'elle a à tout le moins manqué tant à l'obligation à laquelle elle était tenue du fait de son adhésion au service cmnedirect au forfait ouvrant le service de banque en ligne, de consulter attentivement les informations de sécurité accessibles depuis la page d'accueil et mises à jour régulièrement qu'à l'obligation de confidentialité mise à sa charge par les conditions générales de ce produit qui prévoient que le souscripteur est entièrement responsable des conséquences d'une divulgation involontaire à quiconque de ses codes personnels ; qu'elle invoque enfin l'article 3 des conditions générales du porteur de carte bancaire qui imposent au titulaire de la carte de se placer dans un contexte de confidentialité, notamment lors de l'authentification et de veiller à le rester tout au long de l'opération, et ce jusqu'à son terme ; A cet égard que si Madame Y... nie avoir répondu au courriel frauduleux du 25 juillet 2014 et avoir communiqué ses données personnelles, tant bancaires que de téléphonie, cette allégation se trouve contredite par le déroulement et la chronologie des faits comme par la reconnaissance qu'elle en a faite dans ses écritures de première instance aux termes desquelles elle indiquait avoir été victime d'une opération de phishing, encore appelé hameçonnage ou filoutage, technique utilisée par des fraudeurs pour obtenir des renseignements personnels dans le but de perpétrer une usurpation d'identité et qui consiste à faire croire à la victime qu'elle s'adresse à un tiers de confiance, telle qu'une banque ou une administration, afin de lui soutirer des renseignements personnels, tel qu'un mot de passe ou un numéro de carte de crédit ; Que d'ailleurs, c'est, non pas comme elle l'affirme dans ses écritures à la réception de son relevé bancaire le 28 juillet 2014 qu'elle a découvert l'existence de la fraude dont elle indique avoir été victime le 25 juillet précédant, mais bien dès le lendemain matin suivant la réception du courriel frauduleux qu'elle a formé opposition à l'utilisation de sa carte bancaire, ce qui démontre qu'elle éprouvait a minima un doute quant à la provenance dudit message ainsi que la crainte d'avoir fait l'objet d'une tentative d'obtention des données confidentielles relatives à cette carte, et suffit en conséquence à rapporter la preuve qu'elle a bien cliqué sur l'hyperlien mentionné dans le courriel frauduleux qui l'a dirigée vers une page Web sur laquelle elle a été invitée à saisir les informations confidentielles attachées à son compte de téléphonie chez SFR et à sa carte bancaire, permettant ainsi aux fraudeurs de procéder au renvoi des communications arrivant chez elle vers un autre numéro et valider les paiements effectués sur le site marchand en cause ; Que pour autant, outre que la banque ne rapporte pas la preuve d'une absence de défaillance technique ou autre ayant pu affecter les opérations litigieuses, l'examen du courriel reçu par Madame Y... le 25 juillet 2014 révèle que ce dernier provenait de l'adresse mail [...] et portait le logo parfaitement imité de la société SFR, opérateur de téléphonie de Madame Y... ; que son contenu, qui était extrêmement détaillé et dépourvu de faute d'orthographe ou de syntaxe défaillante qui auraient pu alerter Madame Y... sur sa provenance douteuse, était en tout point comparable à un message de rappel de paiement émanant d'une société de ce type ; qu'étaient ainsi notamment rappelées les conséquences encourues par le client en cas de non-paiement de la facture, les diverses modalités de paiement proposées, à savoir par carte bancaire via l'hyperlien « Conso & Factures » ou un numéro de téléphone commençant par 0 806 ou à l'aide d'un TIP, le rappel du numéro 1023 à composer en cas de difficultés, accessible sept jours sur sept de 8 heures à 22 heures ainsi que la mention habituelle, dans ce type de rappel, consistant à préciser au client que s'il vient d'effectuer son règlement, il ne doit pas tenir compte du courrier ; que ce message, comportant un fac

similé de la signature d'une dénommée Valérie A..., présentée comme la directrice de la Relation Client, était en outre suivi du rappel des rubriques de la société SFR «espace client », «assistance », «forum SFR »..., ainsi que des coordonnées complètes de ladite société, numéro de registre du commerce et des sociétés et de taxe sur la valeur ajoutée comprises ; Qu'il suit que ce n'est donc qu'en raison de la confusion entretenue par ce courriel que Madame Y..., qui pensait ainsi procéder au paiement de sa facture SFR, a communiqué à distance les données figurant sur sa carte bancaire et ses données de téléphonie en sorte que c'est véritablement à son insu qu'elle a fourni les renseignements qui ont permis les opérations frauduleuses sur son compte ; Que si un examen minutieux du courriel en question révèle qu'il contenait des indices propres à faire douter de sa provenance, tels que le caractère inadéquat de l'adresse de l'expéditeur, le numéro de contrat SFR mentionné, la discordance entre les montants réclamés ou encore le fait que Madame Y... réglait ses factures de téléphonie par prélèvement bancaire, il n'en demeure pas moins que, dépourvu d'anomalies grossières et revêtant l'apparence générale de l'authenticité, il a surpris la vigilance de Madame Y... en sorte que le fait pour cette dernière d'y avoir répondu ne saurait suffire à caractériser une négligence grave au sens de l'article L. 133-19 précité du code monétaire et financier ; Que dès lors par ailleurs que le litige porte, non pas sur la divulgation des données personnelles de Madame Y... d'accès aux service cmnedirect de consultation et de gestion de compte à distance par Internet, audiotel ou minitel qui permet de consulter le solde des comptes, d'effectuer des virements entre comptes et de réaliser certaines opérations bancaires, mais sur la communication des données attachées à sa seule carte bancaire, la Caisse de Crédit Mutuel de Fruges ne saurait utilement prétendre qu'elle aurait contrevenu aux stipulations destinées à la mettre en garde sur les mesures de sécurité élémentaires qu'elle devait prendre concernant ses données bancaires pour en assurer la confidentialité et en prévenir la divulgation telles que rappelées dans les conditions générales du produit cmnedirect, lesquelles sont sans application en l'espèce ; Que l'invocation, par la banque, des dispositions de l'article 3 des conditions générales du porteur de carte bancaire n'est pas davantage opérante dès lors que si le titulaire d'une carte de paiement doit prendre toute mesure raisonnable pour préserver la sécurité de ses dispositifs de sécurité personnalisés en se plaçant notamment dans un contexte de confidentialité, il n'est pas démontré que Madame Y... n'aurait pas utilisé sa carte de paiement conformément aux conditions régissant sa délivrance et son utilisation, s'agissant d'une opération qu'elle pouvait légitimement penser n'être qu'une opération de paiement à distance ; Qu'il suit de ce qui précède que Madame Y..., qui a notifié sans tarder à la banque le détournement des données liées à l'utilisation de sa carte bancaire et a signalé aux services de gendarmerie la fraude dont elle était victime, est bien fondée à prétendre que les paiements effectués à l'aide des données ainsi subtilisées doivent rester à la charge de la Caisse de Crédit Mutuel de Fruges et à réclamer en conséquence à celle-ci le remboursement des sommes débitées à tort de son compte bancaire au titre de ces paiements frauduleux et qui s'élèvent à la somme non contestée de 6 432,93 euros, sans que la banque puisse lui opposer le plafond de 150 euros prévu à l'article L. 133-19 du code monétaire et financier qui ne joue pas lorsque 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, ni l'absence de dépôt de plainte, cette démarche n'étant pas un préalable au bénéfice de la protection légale prévue par l'article L. 133-19 du code monétaire et financier ; Que la Caisse de Crédit Mutuel de Fruges doit en conséquence, par infirmation du jugement entrepris, être condamnée à rembourser à Madame Y... la somme de 6 432,93 euros, sans que le principe d'une quelconque astreinte ne soit en l'état justifié ; Par ailleurs que dès lors que l'article L. 133-26 du code monétaire et financier interdit, sauf exception, la facturation de toute mesure préventive ou corrective destinée à empêcher ou corriger tout incident dont le client serait victime et qu'en l'absence d'agissement frauduleux de sa part ou de négligence grave, Madame Y... ne saurait supporter aucune conséquence financière résultant de l'utilisation détournée de ses données bancaires, c'est à tort que la Caisse de Crédit Mutuel de Fruges a débité du compte de Madame Y... les frais d'émission d'une nouvelle carte ; qu'il suit que la Caisse de Crédit Mutuel de Fruges doit également être condamnée, par application de l'article L. 133-18 précité du code monétaire et financier, à lui rembourser la somme de 25,90 euros prélevée à ce titre sur son compte bancaire, sans que le principe d'une quelconque astreinte ne soit en l'état davantage justifié ; Que le refus de la banque de supporter les conséquences de la fraude comme elle le devait a causé à Madame Y... un préjudice moral résultant des tracas et désagréments occasionnés qui justifie l'octroi au profit de celle-ci d'une somme de 1 000 euros de dommages et intérêts ; Enfin qu'il apparaît inéquitable de laisser à la charge de Madame Y... les frais exposés par elle tant en première instance qu'en cause d'appel et non compris dans les dépens ; qu'il lui sera en conséquence alloué, à la charge de la Caisse de Crédit Mutuel de Fruges, la somme de 1 500 euros au titre de l'article 700 du code de procédure civile ; Qu'il apparaît par ailleurs équitable de faire supporter par Madame Y..., au titre des frais exposés tant en première instance qu'en cause d'appel par la Caisse Fédérale de Crédit Mutuel Nord Europe et non compris dans les dépens, la somme de 300 euros » ;

1°) ALORS QUE l'utilisateur d'un service de paiement qui agit avec une négligence grave est tenu de supporter l'intégralité

de la perte subie ; que constitue une négligence grave la fourniture par le client d'un établissement bancaire à un tiers de données confidentielles dont il a contractuellement la charge de la conservation, ayant permis ou facilité l'utilisation d'un service de paiement sécurisé ; qu'en l'espèce, il résulte de l'arrêt attaqué (p. 6, 2ème et 3ème §) que, contrairement à ce qu'elle prétendait, Madame Y... avait répondu à un courriel frauduleux qu'elle avait reçu le 25 juillet 2014, et avait communiqué à cette occasion les données confidentielles ayant permis aux fraudeurs d'effectuer les paiements litigieux ; que, pour juger néanmoins que Madame Y... n'avait pas commis de négligence grave dans la conservation de ses données personnelles, la cour d'appel a retenu que le courriel reçu par Madame Y... provenait de l'adresse mail [...] et portait le logo parfaitement imité de la société SFR, opérateur de téléphonie de Madame Y..., que son contenu, qui était détaillé et dépourvu de faute d'orthographe ou de syntaxe défaillante qui auraient pu alerter Madame Y..., était en tout point comparable à un message de rappel de paiement émanant d'une société de ce type ; qu'elle a en outre considéré que si un examen minutieux du courriel en question révélait qu'il contenait des indices propres à faire douter de sa provenance, tels que le caractère inadéquat de l'adresse de l'expéditeur, le numéro de contrat SFR mentionné, la discordance entre les montants réclamés ou encore le fait que Madame Y... réglait ses factures de téléphonie par prélèvement bancaire, il n'en demeurait pas moins que, dépourvu d'anomalies grossières et revêtant l'apparence générale de l'authenticité, il avait surpris la vigilance de Madame Y..., ce dont elle a déduit que le fait pour cette dernière d'y avoir répondu ne saurait suffire à caractériser une négligence grave au sens de l'article L. 133-19 précité du code monétaire et financier ; qu'en statuant de la sorte, quand il résultait de ses propres constatations que Madame Y... avait fourni à un tiers l'ensemble des données personnelles permettant l'utilisation du système de paiement 3D SECURE ainsi que d'effectuer des virements sur internet, ce qui caractérisait une négligence grave dans la conservation de ses données personnelles, la cour d'appel a violé les articles L. 133-15, L. 133-16, L. 133-19 et L. 133-23 du code monétaire et financier, ensemble l'article 1134 du code civil ;

2°) ALORS, EN TOUT ETAT DE CAUSE, QUE la cour d'appel a constaté qu' « un examen minutieux du courriel en question rév[élait] qu'il contenait des indices propres à faire douter de sa provenance, tels que le caractère inadéquat de l'adresse de l'expéditeur, le numéro de contrat SFR mentionné, la discordance entre les montants réclamés ou encore le fait que Madame Y... réglait ses factures de téléphonie par prélèvement bancaire » ; qu'en jugeant néanmoins qu'en dépit de ces incohérences qui auraient pourtant dû alerter toute personne normalement prudente et avisée, Madame Y... avait légitimement pu croire, en fournissant ses données confidentielles en réponse à ce courriel, qu'elle procédait à une simple opération de paiement à distance, la cour d'appel n'a pas tiré les conséquences légales de ses propres constatations, violant ainsi les articles L. 133-15, L. 133-16 et L. 133-19 du code monétaire et financier ;

3°) ALORS QUE comme le faisait valoir la Caisse de Crédit Mutuel de FRUGES dans ses écritures d'appel (spéc. p. 7), et l'a relevé la cour d'appel (p. 7, 1er §), il existait dans le mail reçu le 25 juillet 2014 par Madame Y... une discordance entre le montant indiqué comme impayé sur l'en-tête du mail du 25 juillet 2014 (« 19,99 ? TTC ») et le montant mentionné dans le texte du courriel « Nous constatons que votre compte présente toujours un solde débiteur de 15,99 ? TTC ») ; qu'en outre, le montant de la prétendue dette de Madame Y... n'était pas libellée avec le symbole de l'euro (« € ») mais comportait un point d'interrogation ; que l'arrêt constate en outre que le numéro de contrat SFR indiqué n'était pas celui de Madame Y... ; qu'en énonçant que le courriel en question était « dépourvu d'anomalies grossières et revêta[it] l'apparence générale de l'authenticité », la cour d'appel a dénaturé le courriel du 25 juillet 2014, violant l'article 1134 du code civil (nouvel article 1192 du code civil), ensemble l'interdiction faite aux juges de dénaturer les documents de la cause ;

4°) ALORS QUE la cour d'appel a expressément constaté, d'une part, qu'il résultait du rapport du service fonction monétique du Crédit Mutuel que les opérations d'achat litigieuses avaient été réalisées à partir de deux adresses IP distinctes et que les codes à usage unique ayant servi à valider chacun des sept achats litigieux après communication des données attachées à la carte bancaire de Madame Y... avaient été adressés via le serveur vocal interactif de la banque sur un numéro de téléphone fixe dont il n'est pas contesté qu'il s'agit de celui de Madame Y..., de sorte que la Caisse de Crédit Mutuel de Fruges rapportait ainsi la preuve, conformément à l'article L. 133-23 précité du code monétaire et financier, que les opérations de paiement contestées avaient été authentifiées, dûment enregistrées et comptabilisées (arrêt, p. 5, 4ème et 5ème §), et d'autre part, que la preuve était rapportée que Madame Y... « a[vait] bien cliqué sur l'hyperlien mentionné dans le courriel frauduleux qui l'a dirigée vers une page Web sur laquelle elle a été invitée à saisir les informations confidentielles attachées à son compte de téléphonie chez SFR et à sa carte bancaire, permettant ainsi aux fraudeurs de procéder au renvoi des communications arrivant chez elle vers un autre numéro et valider les

paiements effectués sur le site marchand en cause » (p. 6, 3ème §) ; qu'en relevant incidemment, pour faire droit aux demandes en remboursement et indemnitaires de Madame Y..., que « la banque ne rapporte pas la preuve d'une absence de défaillance technique ou autre ayant pu affecter les opérations litigieuses », quand il résultait de ses propres constatations que le Crédit Mutuel établissait que les opérations litigieuses avaient été dûment enregistrées et que la réalisation des opérations de paiement en cause avait été permise par la communication de ses données confidentielles par Madame Y... à un tiers mal intentionné, la cour d'appel a violé les articles L. 133-19 et L. 133-23 du code monétaire et financier ;

5°) ALORS, TRES SUBSIDIAIREMENT, QUE la commission par l'utilisateur d'un service de paiement d'une négligence grave au sens de l'article L. 133-19 IV du code monétaire et financier entraîne à tout le moins un partage de responsabilité entre ce dernier et la banque qui n'établirait pas l'absence de déficience technique du système de paiement qu'elle a mis en place ; qu'en faisant droit en son entier à la demande de remboursement de Madame Y..., quand il résultait de ses constatations que cette dernière avait commis une négligence grave dans la conservation de ses données confidentielles, justifiant à tout le moins un partage de responsabilité avec le Crédit Mutuel, la cour d'appel a encore violé les articles L. 133-19 et L. 133-23 du code monétaire et financier.

Décision **attaquée**

Cour d'appel de douai chambre 8 section 1
3 novembre 2016 (n°16/00233)

VOIR LA DÉCISION