Le : 10/02/2017

Cour de cassation

chambre commerciale

Audience publique du 18 janvier 2017

N° de pourvoi: 15-26058

ECLI:FR:CCASS:2017:CO00110

Non publié au bulletin

Rejet

Mme Mouillard (président), président

SCP Célice, Soltner, Texidor et Périer, SCP Ortscheidt, avocat(s)

REPUBLIQUE FRANCAISE

AU NOM DU PEUPLE FRANCAIS

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

Sur le moyen unique, pris en deux premières branches :

Attendu, selon l'arrêt attaqué (Douai, 3 septembre 2015), que M. X..., titulaire de deux comptes dans les livres de la société Caisse de crédit mutuel d'Hellemmes (la Caisse), a contesté plusieurs opérations de paiement, effectuées, selon lui, frauduleusement sur ces comptes, 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 donnant à un tiers des informations confidentielles permettant d'effectuer les opérations contestées, M. X... l'a assignée en remboursement des sommes débitées sur ses comptes et en paiement de dommages-intérêts ;

Attendu que la Caisse fait grief à l'arrêt d'accueillir ces demandes alors, selon le moyen :

1°/ 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 la circonstance qu'un instrument de paiement ait été utilisé pour des achats sur le réseau internet par utilisation de données ne se trouvant pas sur la carte de paiement proprement dite, tels des clefs personnelles permettant au titulaire du compte de venir authentifier le paiement au moyen d'une donnée

confidentielle, ainsi que le numéro de téléphone ou l'adresse électronique du client, destiné à recevoir de la banque un code de confirmation permettant de réaliser le paiement souhaité, démontre à elle-seule la négligence grave du titulaire dans la conservation des données sécurisées de paiement que lui imposent les dispositions de l'article L. 133-16, alinéa 1er, du code monétaire et financier ; qu'en l'espèce, la Caisse faisait valoir que le système de paiement à distance « payweb », utilisé pour réaliser les débits contestés par M. X..., comportait un processus hautement sécurisé nécessitant le choix par le client d'un identifiant et d'un mot de passe lors de la première connexion, puis, pour la réalisation de chaque opération de paiement, la création d'une carte « payweb » par un dispositif de « clefs personnelles » permettant à l'utilisateur de choisir une combinaison de chiffres au sein d'une carte de 64 codes, avant que la banque n'envoie, par mail ou un sms, un code de confirmation à validité temporaire permettant d'effectuer le paiement désiré ; que pour condamner la Caisse à prendre en charge le remboursement de débits effectués sur le compte de M. X... par le biais du service « payweb », la cour d'appel, après avoir retenu que les données bancaires de M. X... avaient été détournées à l'insu de ce dernier, a considéré que la banque ne pouvait démontrer la négligence grave de M. X... du seul fait de la création et de l'utilisation par un tiers des cartes de paiement virtuelles litigieuses avec tabulation des données bancaires personnelles ; qu'en statuant de la sorte, quand la circonstance, constatée par l'arrêt que les débits litigieux avaient été effectués par le biais d'un service de paiement sécurisé nécessitant la fourniture de données strictement personnelles à M. X..., et dont ce dernier avait contractuellement la charge d'assurer la conservation et la confidentialité, impliquait que ce dernier avait commis une négligence grave dans la conservation des dites données, la cour d'appel a méconnu les articles L. 133-15, L. 133-16 et L. 133-19 du code monétaire et financier, ensemble l'article 1134 du code civil ;

2°/ que la circonstance qu'un service de paiement doté d'un dispositif de sécurité ait été utilisé pour des achats sur le réseau internet par utilisation d'un l'identifiant internet et du mot de passe de connexion, des clefs personnelles permettant à l'utilisateur de venir authentifier le paiement au moyen d'une donnée confidentielle ne se trouvant pas sur la carte de paiement proprement dite, ainsi que de l'adresse électronique du client aux fins de réception du code de confirmation permettant l'achat, fait à tout le moins présumer le défaut de garde des données confidentielles d'instrument de paiement et la négligence grave de son utilisateur dans la préservation de la confidentialité de ses données personnelles ; qu'il appartient dans ces circonstances à l'utilisateur du service de paiement de rapporter par tous moyens la preuve qu'il a respecté son obligation de conserver les données confidentielles permettant l'utilisation du service qui lui a été proposé ; qu'en jugeant que la banque ne pouvait démontrer la négligence grave de M. X... du seul fait de la création et de l'utilisation par un tiers des cartes de paiement virtuelles litigieuses avec tabulation des données bancaires personnelles, quand la circonstance que les débits litigieux avaient été effectués par le biais d'un service de paiement sécurisé nécessitant la fourniture de données strictement personnelles à M. X..., et dont ce dernier avait contractuellement la charge d'assurer la conservation et la confidentialité, faisait présumer la négligence grave de l'utilisateur dans la conservation de ses données personnelles, la cour d'appel a violé les articles L. 133-15, L. 133-16 et L. 133-19 du code monétaire et financier, ensemble l'article 1134 du code civil ;

Mais attendu que si, aux termes des articles L. 133-16 et L. 133-17 du code monétaire et financier, il appartient à l'utilisateur de services de paiement de prendre toute mesure raisonnable pour préserver la sécurité de ses dispositifs de sécurité personnalisés et

d'informer sans tarder son prestataire de tels services de toute utilisation non autorisée de l'instrument de paiement ou des données qui lui sont liées, c'est à ce prestataire qu'il incombe, par application des articles L. 133-19, IV, et L. 133-23 du même code, de rapporter la preuve que l'utilisateur, qui nie avoir autorisé une opération de paiement, a agi frauduleusement ou n'a pas satisfait, intentionnellement ou par négligence grave, à ses obligations ; que cette preuve ne peut se déduire du seul fait que l'instrument de paiement ou les données personnelles qui lui sont liées ont été effectivement utilisés ; qu'ayant souverainement retenu qu'au soutien de son allégation selon laquelle M. X... avait révélé volontairement à un tiers ses données bancaires, et notamment son identifiant « CMNE Direct », le mot de passe associé et les codes de validation présents sur sa carte d'authentification renforcée, ou que, par négligence, il avait permis à un tiers d'en prendre aisément connaissance, la Caisse se bornait à affirmer que M. X... avait vraisemblablement été victime d'un « hameçonnage », se contentant à cet égard de procéder par simple voie de supputations impropres à caractériser une imprudence de son client, c'est exactement que la cour d'appel a accueilli la demande de remboursement de M. X... ; que le moyen n'est pas fondé ;

Et attendu qu'il n'y a pas lieu de statuer par une décision spécialement motivée sur le moyen, pris en ses trois dernières branches, qui n'est manifestement pas de nature à entraîner la cassation ;

PAR CES MOTIFS :

REJETTE le pourvoi ;

Condamne la société Caisse de crédit mutuel d'Hellemmes aux dépens ;

Vu l'article 700 du code de procédure civile, rejette sa demande et la condamne à payer à M. X... la somme de 3 000 euros ;

Ainsi fait et jugé par la Cour de cassation, chambre commerciale, financière et économique, et prononcé par le président en son audience publique du dix-huit janvier deux mille dix-sept.

MOYEN ANNEXE au présent arrêt

Moyen produit par la SCP Célice, Soltner, Texidor et Périer, avocat aux Conseils, pour la société Caisse de crédit Mutuel d'Hellemmes

Il est fait grief à l'arrêt attaqué D'AVOIR condamné la CAISSE DE CRÉDIT MUTUEL D'HELLEMMES à payer à Monsieur Manuel X... la somme de 5. 183, 14 € au titre des prélèvements frauduleux effectué sur ses comptes bancaires, D'AVOIR condamné la

CAISSE DE CRÉDIT MUTUEL D'HELLEMMES à payer à Monsieur Manuel X... la somme de 690, 55 euros au titre des frais bancaires, et D'AVOIR condamné la CAISSE DE CRÉDIT MUTUEL D'HELLEMMES à payer à Monsieur Manuel X... la somme de 1. 000 euros à titre de dommages et intérêts ;

AUX MOTIFS PROPRES QUE « selon le paragraphe II de l'article L. 133-19 du code monétaire et financier, 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. 33-20 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 ; Attendu qu'il n'est pas contesté que l'utilisation du service de banque à distance nécessite la saisie successive de l'identifiant CMNE du client, d'un mot de passe personnel à l'utilisateur attaché à cet identifiant, d'un code de validation à quatre chiffres présent sur une carte d'authentification renforcée comportant soixante-quatre combinaisons remise au client pour effectuer certains opérations comme la modification des coordonnées personnelles ou la création de cartes payweb et la validation de l'opération par un code de confirmation envoyé soit par mail soit par SMS au sociétaire après la saisie de son code de carte d'authentification ; Attendu qu'avisée de la contestation de Monsieur Manuel X... qui nie être l'auteur d'opérations de paiements effectués les 25 et 28 mai 2013 à partir de cartes virtuelles PAYWEB générées à partir de ses deux cartes de crédit MASTERCARD, la CAISSE DE CRÉDIT MUTUEL D'HELLEMMES 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 ; Attendu ainsi que le rapport du service des fraudes et affaires spéciales de la banque a permis d'établir que dix commandes de cartes virtuelles PAY WEB d'une durée de validité

de 15 minutes et d'un montant de 500 euros chacune ont été enregistrées, cinq via la carte Mastercard n° 5132720194885847 appartenant à Monsieur Manuel X... le 25 mai 2013 à 12 heures 01, 12 heures 02, 12 heures 03, 12 heures 04, 12 heures 05, et cinq via la carte Mastercard n° 5132720193687269 appartenant à Monsieur Manuel X... le 25 mai 2013 à 12 heures 07, 12 heures 09, 12 heures 10, 12 heures 11, 12 heures 12 ; Que deux autres commandes de carte virtuelle d'un montant de 200 euros pour la première et de 90 euros pour la seconde ont en outre été enregistrées le 28 mai 2013, à 2 heures 58 via la carte Mastercard n° 5132720193687269 de Monsieur Manuel X... et à 19 heures 30 via la carte Mastercard n° 5132720194885847 de ce dernier ; Qu'alors que pour les commandes réalisées le 25 mai 2013 et le 28 mai à 2 heures 58, l'adresse IP utilisée pour se connecter à la banque à distance portait le numéro 134. 255. 247. 107 permettant ainsi de la localiser en Allemagne, celle utilisée le 28 mai à 19 heures 30 suivant portait le numéro 94. 23. 51. 223 correspondant à une adresse en France ; Qu'il apparaît en outre que d'autres adresses IP ont été utilisées pour des tentatives, l'une ressortant comme privée et l'autre comme située à Paris ; Qu'à l'exception de la carte virtuelle créée le 28 mai 2012 à 19 heures 30 d'un montant de 90 euros qui n'a finalement pas été utilisée, toutes les autres cartes ont permis d'effectuer des achats auprès de l'enseigne PAYTOP à Paris pour un montant total de 4 983, 14 euros et auprès de l'enseigne LA CASE A WILLY à Rivière Pilote en Martinique pour 200 euros ; Qu'il ressort en outre de ce rapport que la création des payweb cards emportant attribution d'un numéro virtuel à seize chiffres, a été validée, pour chacune, par la saisie de l'identifiant de Monsieur Manuel X..., de son mot de passe associé et du code renforcé indiqué sur sa carte de clés personnelles ; Que le code de confirmation à six chiffres, associé à une date de validité et un cryptogramme visuel à trois chiffres, permettant de générer le numéro virtuel attaché à chacune de ces cartes de paiement virtuelles, a été, à chaque reprise, transmis à l'adresse mail skychfal @ hotmail. com qui n'est pas l'adresse mail habituellement enregistrée par Monsieur Manuel X... sur le site de la banque ; qu'aucune précision n'est en revanche fournie par la banque relativement aux date et heure auxquelles cette modification, qui, selon les conditions générales versées aux débats, a elle-même nécessité la saisie de l'identifiant, du mot de passe associé et du code renforcé indiqué sur sa carte de clés personnelles, est intervenue ; Que pour réaliser les paiements sur le site marchand ont été successivement saisis le numéro de la carte à seize chiffres, la date de fin de validité et un cryptogramme visuel à trois chiffres ; Attendu que le détournement, à l'insu de Monsieur Manuel X..., de ses données bancaires personnelles et des cartes virtuelles générées à partir de ses cartes de crédit MASTERCARD n'est pas contesté par la CAISSE DE CRÉDIT MUTUEL D'HELLEMMES et est au demeurant suffisamment établi par les circonstances entourant la création et l'utilisation des cartes bancaires virtuelles litigieuses ; Qu'il suit que Monsieur Manuel X..., dont il apparaît à la lecture de l'historique des autorisations cartes qu'il produit aux débats qu'il se trouvait en Belgique le 25 mai 2013 pour y avoir procédé à divers paiements au moyen de l'une de ses deux cartes de crédit MASTERCARD, est bien fondé à demander le bénéfice des dispositions précitées du code monétaire et financier, sauf à se voir opposer la négligence grave dont il se serait rendu coupable en divulguant ses données bancaires personnelles ; Attendu à cet égard que si conformément à l'article L. 133-23 précité du code monétaire et financier, la CAISSE DE CRÉDIT MUTUEL D'HELLEMMES rapporte la preuve que les opérations de paiements contestées ont été authentifiées, dûment enregistrées et comptabilisées et qu'elles n'ont pas été affectées par une déficience technique ou autre, il n'en demeure pas moins que les utilisations successives du service de paiement PAYWEB CARDS telles qu'enregistrées par la banque ne suffisent pas nécessairement en tant que telles à prouver que les opérations ont été autorisées par Monsieur Manuel X... ou que celui-ci n'a pas satisfait intentionnellement ou par négligence grave aux obligations lui incombant en la matière ; Qu'il suit que la CAISSE DE CRÉDIT MUTUEL D'HELLEMMES, prestataire du service de

paiement incriminé, ne peut, du seul fait de la création et de l'utilisation par un tiers des cartes de paiement virtuelles litigieuses avec tabulation des données bancaires personnelles de Monsieur Manuel X..., éléments nécessaires pour créer lesdites cartes puis valider les paiements, prétendre démontrer une négligence grave de son client au sens de l'article L. 311-19 précité ; Que c'est en conséquence à elle de démontrer que Monsieur Manuel X... a révélé volontairement à un tiers ses données bancaires et notamment son identifiant CMNE DIRECT, le mot de passe associé et les codes de validation présents sur sa carte d'authentification renforcée, ou démontrer que par négligence, ce dernier a permis à un tiers d'en prendre aisément connaissance ; Que si la CAISSE DE CRÉDIT MUTUEL D'HELLEMMES affirme à cet égard que Monsieur Manuel X... a vraisemblablement été victime de faits d'hameçonnage, elle n'en rapporte nullement la preuve, se contentant à cet égard de procéder par simple voie de supputations impropres à caractériser une imprudence de son client à l'origine des paiements litigieux alors d'une part que l'association de consommateurs Que Choisir soupçonne une brèche dans le dispositif de sécurité de la banque, le portail PAYWEB étant suspecté d'être facilement mis en échec par les pirates informatiques, que la carte d'authentification renforcée peut être commandée par internet après la simple saisie de l'identifiant et du mot de passe associé et que l'actualité récente fait état de plusieurs cas dans lesquels des malfaiteurs sont parvenus à s'approprier des données bancaires confidentielles d'accès aux services de consultation et de gestion de compte à distance par internet sans pour autant bénéficier de la négligence voire de la complicité du titulaire de ladite carte ; Qu'à défaut de rapporter la preuve que Monsieur Manuel X... aurait, même involontairement, divulgué ses codes personnels et plus généralement ses données personnelles et confidentielles à un tiers, la CAISSE DE CRÉDIT MUTUEL D'HELLEMMES ne saurait prétendre que Monsieur Manuel X... aurait contrevenu aux stipulations destinées à le mettre en garde sur les mesures de sécurité élémentaires qu'il 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 CMNE DIRECT, étant au demeurant en tout état de cause observé que la banque ne fournit pas les conditions générales en vigueur au jour de l'adhésion de son client au produit ni ne justifie d'une acceptation expresse de modifications postérieures ; Qu'elle ne peut donc, sans preuve de la mauvaise foi de Monsieur Manuel X..., client, s'opposer au remboursement des sommes qu'elle a indûment débitées des comptes de celui-ci au titre des opérations de paiement effectuées à l'aide des cartes PAYWEB litigieuses ; Attendu qu'aucune négligence grave de la part de Monsieur Manuel X... au regard des dispositions précitées de l'article L. 133-16 du code monétaire et financier n'étant en ces conditions établie, le jugement doit être confirmé en ce qu'il a condamné la CAISSE DE CREDIT MUTUEL D'HELLEMMES à rembourser à Monsieur Manuel X... les sommes débitées à tort de ses comptes bancaires ; Attendu qu'à cet égard c'est à bon droit que le premier juge a chiffré le montant total de ces sommes, non pas à la valeur intrinsèque des cartes bancaires virtuelles créées sans autorisation, mais au total des paiements effectués au moyen de ces cartes, soit une somme de 5 183, 14 euros, Attendu par ailleurs que dès lors qu'en l'absence d'agissement frauduleux de sa part ou de négligence grave, Monsieur Manuel X... ne saurait supporter aucune conséquence financière résultant de l'utilisation détournée de ses données bancaires, la CAISSE DE CREDIT MUTUEL D'HELLEMMES doit également, par application de l'article L. 133-18 précité du code monétaire et financier, être condamnée à lui rembourser l'intégralité des frais bancaires liés à la fraude dont il a été victime ; Que la CAISSE DE CRÉDIT MUTUEL D'HELLEMMES ne formulant aucune critique sur les modalités de calcul des sommes dues par elle à ce titre, elle sera donc, par infirmation du jugement déféré, condamnée à régler à Monsieur Manuel X... une somme complémentaire de 690, 55 euros ; Attendu par ailleurs qu'il n'est pas contesté que la CAISSE DE CRÉDIT MUTUEL D'HELLEMMES a déclaré Monsieur Manuel X... au

fichier national des incidents de paiement de la Banque de France au titre du solde débiteur de son compte non régularisé ; qu'il n'est pas davantage contesté que c'est à la suite des opérations frauduleuses, dont Monsieur Manuel X... a été victime en mai 2013, que son compte est devenu débiteur et qu'il n'a pas été régularisé en raison du refus de la banque de prendre en charge le montant du sinistre sans motif légitime ; Que le refus de la banque de supporter les conséquences de la fraude comme elle le devait a causé à Monsieur Manuel X... un préjudice moral résultant de son inscription au fichier des incidents de paiement de la Banque de France avec toutes les conséquences que cela comporte en terme de solvabilité et de réputation bancaire qui justifie l'octroi au profit de celui-ci d'une somme de 1 000 euros de dommages et intérêts ; Attendu enfin qu'il apparaît inéquitable de laisser à la charge de Monsieur Manuel X... les frais exposés par lui en cause d'appel et non compris dans les dépens ; qu'il lui sera en conséquence alloué la somme de 1 500 euros au titre de l'article 700 du code de procédure civile, l'indemnité allouée en première instance étant confirmée » ;

ET AUX MOTIFS SUPPOSEMENT ADOPTES DU JUGEMENT ENTREPRIS QUE « Sur la demande principale de Monsieur Manuel X... : L'article L133-19 du code monétaire, et financier prévoit en son point II que la responsabilité du payeur n'est pas engagée si l'opération de paiement non autorisée a été effectuée en détournant, à son insu, l'instrument de paiement ou les données qui lui sont liées. Le point IV du même article dispose 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 L133-16 et L 133-17. La Banque doit donc démontrer que le porteur a révélé volontairement à un tiers ses données personnelles ou démontrer que par une négligence grave, il a permis à un tiers d'en prendre aisément connaissance. Sur ce : LA CAISSE DE CRÉDIT MUTUEL DE HELLEMMES ne procède que par voie de suppositions en indiquant que Monsieur Manuel X... aurait été destinataire d'un courriel frauduleux l'invitant à compléter un formulaire en ligne avec des informations confidentielles qu'il aurait effectivement communiquées au fraudeur, mais n'en apporte pas la preuve. Il ne ressort pas d'autres éléments du dossier que ceux résultant des propres affirmations de LA CAISSE DE CRÉDIT MUTUEL DE HELLEMMES que Monsieur Manuel X... aurait communiqué ses données personnelles en commettant ainsi une négligence grave qui serait seule à l'origine de son préjudice. Il est observé par ailleurs que les opérations litigieuses se sont, pour la plupart, succédées à environ une minute d'intervalle, ce qui rend peu vraisemblable l'utilisation par le fraudeur de l'ensemble des codes des systèmes de sécurité de PAYWEB, puisqu'il aurait fallu, en une minute environ, qu'il saisisse l'ensemble des données de confidentialité avant d'opérer un autre achat en ligne dans la foulée, ce qui semble matériellement impossible. Monsieur Manuel X... justifie avoir été normalement diligent en formant opposition le 29 mai, en déposant une réclamation le 30 mai et en se présentant aux services de police pour déclarer l'utilisation frauduleuse de sa carte de paiement le 31 mai. En l'absence de toute faute ou négligence gave de sa part, il y a lieu de faire droit à sa demande d'indemnisation au titre des sommes prélevées sur ses comptes par fraude, soit la somme de 5, 183, 14 euros selon la pièce n° 20 de LA CAISSE DE CRÉDIT MUTUEL DE HELLEMMES, Monsieur Manuel X... ne produisant pas ses relevés de compte et n'établissant pas que les prélèvements litigieux auraient été supérieurs à cette somme. Les intérêts légaux seront dus à compter de la mise en demeure reçue le 10/ 10/ 2013. LA CAISSE DE CRÉDIT MUTUEL DE HELLEMMES sera donc condamnée au paiement de ces sommes à Monsieur Manuel X..., et sous astreinte de 50 euros par jour de retard passé le délai d'un mois à compter du jour où la décision sera devenue définitive. Sur les frais bancaires : Il

appartient à chaque partie d'apporter les éléments de preuve nécessaires au succès de ses prétentions. Monsieur Manuel X... indique que LA CAISSE DE CRÉDIT MUTUEL DE HELLEMMES aurait prélevé des frais sur ses comptes suite aux incidents de paiement ayant découlé des opérations frauduleuses, mais n'en apporte pas la preuve, alors que la simple production de ses relevés de compte aurait permis de constater les éventuels frais prélevés par la banque. Il sera donc débouté de ce chef de demande. Sur la demande de dommages et intérêts de Monsieur Manuel X... pour intimidation et résistance abusive : Il est'établi que malgré des tentatives d'accord amiable de la part de Monsieur Manuel X... et des courriers de son conseil, et alors même que c'est la banque ellemême qui avait averti Monsieur Manuel X..., qu'il y avait eu des opérations qui semblaient frauduleuses sur ses comptes, LA CAISSE DE CRÉDIT MUTUEL DE HELLEMMES a effectué les démarches pour son inscription au FICP. Il en est résulté pour Monsieur Manuel X... un préjudice moral mais aussi un trouble dans les conditions d'existence qui sera indemnisé à hauteur de 500 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 la circonstance qu'un instrument de paiement ait été utilisé pour des achats sur le réseau internet par utilisation de données ne se trouvant pas sur la carte de paiement proprement dite, tels des clefs personnelles permettant au titulaire du compte de venir authentifier le paiement au moyen d'une donnée confidentielle, ainsi que le numéro de téléphone ou l'adresse électronique du client, destiné à recevoir de la banque un code de confirmation permettant de réaliser le paiement souhaité, démontre à elle-seule la négligence grave du titulaire dans la conservation des données sécurisées de paiement que lui imposent les dispositions de l'article L. 133-16, alinéa 1er, du code monétaire et financier ; qu'en l'espèce, la Caisse de Crédit Mutuel de LILLE HELLEMES faisait valoir (ses conclusions d'appel, p. 3 à 5) que le système de paiement à distance « payweb », utilisé pour réaliser les débits contestés par Monsieur X..., comportait un processus hautement sécurisé nécessitant le choix par le client d'un identifiant et d'un mot de passe lors de la première connexion, puis, pour la réalisation de chaque opération de paiement, la création d'une carte « payweb » par un dispositif de « clefs personnelles » permettant à l'utilisateur de choisir une combinaison de chiffres au sein d'une carte de 64 codes, avant que la banque n'envoie, par mail ou un sms, un code de confirmation à validité temporaire permettant d'effectuer le paiement désiré ; que pour condamner la Caisse de Crédit Mutuel de LILLE HELLEMES à prendre en charge le remboursement de débits effectués sur le compte de Monsieur X... par le biais du service « payweb », la Cour d'appel, après avoir retenu que les données bancaires de Monsieur X... avaient été détournées à l'insu de ce dernier (arrêt, p. 6, 2ème §), a considéré que la banque ne pouvait démontrer la négligence grave de Monsieur X... du seul fait de la création et de l'utilisation par un tiers des cartes de paiement virtuelles litigieuses avec tabulation des données bancaires personnelles ; qu'en statuant de la sorte, quand la circonstance, constatée par l'arrêt (p. 4, avant-dernier §) que les débits litigieux avaient été effectués par le biais d'un service de paiement sécurisé nécessitant la fourniture de données strictement personnelles à Monsieur X..., et dont ce dernier avait contractuellement la charge d'assurer la conservation et la confidentialité, impliquait que ce dernier avait commis une négligence grave dans la conservation desdites données, la Cour d'appel a méconnu les articles L. 133-15, L. 133-16 et L. 133-19 du code monétaire et financier, ensemble l'article 1134 du code civil ;

2°) ALORS, EN TOUT ETAT DE CAUSE, QUE la circonstance qu'un service de paiement doté d'un dispositif de sécurité ait été utilisé pour des achats sur le réseau internet par

utilisation d'un l'identifiant internet et du mot de passe de connexion, des clefs personnelles permettant à l'utilisateur de venir authentifier le paiement au moyen d'une donnée confidentielle ne se trouvant pas sur la carte de paiement proprement dite, ainsi que de l'adresse électronique du client aux fins de réception du code de confirmation permettant l'achat, fait à tout le moins présumer le défaut de garde des données confidentielles d'instrument de paiement et la négligence grave de son utilisateur dans la préservation de la confidentialité de ses données personnelles ; qu'il appartient dans ces circonstances à l'utilisateur du service de paiement de rapporter par tous moyens la preuve qu'il a respecté son obligation de conserver les données confidentielles permettant l'utilisation du service qui lui a été proposé ; qu'en jugeant que la banque ne pouvait démontrer la négligence grave de Monsieur X... du seul fait de la création et de l'utilisation par un tiers des cartes de paiement virtuelles litigieuses avec tabulation des données bancaires personnelles, quand la circonstance que les débits litigieux avaient été effectués par le biais d'un service de paiement sécurisé nécessitant la fourniture de données strictement personnelles à Monsieur X..., et dont ce dernier avait contractuellement la charge d'assurer la conservation et la confidentialité, faisait présumer la négligence grave de l'utilisateur dans la conservation de ses données personnelles, la Cour d'appel a violé les articles L. 133-15, L. 133-16 et L. 133-19 du code monétaire et financier, ensemble l'article 1134 du code civil ;

3°) ALORS QU'il était stipulé dans les conditions particulières du contrat EUROCOMPTE DUO CONFORT n° 00019583208 signé par Monsieur X... le 25 novembre 2009, régulièrement produit aux débats par la Caisse de Crédit Mutuel de LILLE HELLEMES (pièce n° 1 de son bordereau de communication de pièces), que « pour accéder au service choisi, utiliser l'identification suivante : 0271119583208. Le souscripteur reconnait avoir reçu de manière individuelle, sur un document séparé, son mot de passe. Le souscripteur s'engage à se connecter immédiatement au service choisi pour en modifier le mot de passe. Le souscripteur reconnait le caractère confidentiel et personnel de l'identifiant et du mot de passe et s'engage à les mettre en sécurité. Dès sa prochaine connexion à cmnedirect au forfait via internet, puis fréquemment il s'engage également à consulter attentivement les informations de sécurité accessibles depuis la page d'accueil et mises à jour, régulièrement » ; que pour juger que la Caisse de Crédit Mutuel de LILLE HELLEMES ne justifiait pas que Monsieur X... avait contrevenu aux stipulations destinées à le mettre en garde sur les mesures de sécurité élémentaires qu'il devait prendre concernant ses données bancaires pour en assurer la confidentialité et en prévenir la divulgation, la Cour d'appel a incidemment retenu qu'en tout état de cause, la banque ne fournissait pas « les conditions générales en vigueur au jour de l'adhésion de son client au produit ni ne justifie d'une acceptation expresse de modifications postérieures » ; qu'en statuant de la sorte, sans rechercher, comme elle y était invitée, si l'obligation pour Monsieur X... d'assurer la sécurité de ses données personnelles ne résultait pas des conditions particulières du contrat, la Cour d'appel a privé sa décision de base légale au regard de l'article 1134 du code civil ;

4°) ALORS, EN OUTRE, QUE le juge ne peut statuer ni par des motifs hypothétiques, ni par des motifs d'ordre général dépourvus d'assise dans les faits de la cause ; qu'en retenant, pour juger qu'il n'était pas démontré que Monsieur X... avait commis une négligence grave dans la conservation de ses données personnelles, à l'origine des débits litigieux, que l'association de consommateurs Que Choisir « soupçonn [ait] une brèche dans le dispositif de sécurité de la banque, le portail PAYWEB étant suspecté d'être facilement mis en échec par les pirates informatiques », et que la carte d'authentification

renforcée pouvait être commandée par internet après la simple saisie de l'identifiant et du mot de passe associé et que l'actualité récente faisait état de plusieurs cas dans lesquels des malfaiteurs sont parvenus à s'approprier des données bancaires confidentielles d'accès aux services de consultation et de gestion de compte à distance par internet sans pour autant bénéficier de la négligence voire de la complicité du titulaire de ladite carte, la Cour d'appel, qui a statué par des motifs hypothétiques et généraux, impropres à justifier sa décision, a violé l'article 455 du code de procédure civile ;

5°) ALORS EN TOUT ETAT DE CAUSE QUE les juges ne peuvent accueillir ou rejeter les demandes dont ils sont saisis sans examiner les éléments de preuve fournis par les parties au soutien de leurs prétentions ; qu'en l'espèce, le tribunal d'instance, pour juger qu'il n'était pas établi que Monsieur X... avait commis une négligence grave dans la conservation de ses données personnelles, et en particulier écarter l'hypothèse d'un « phishing », a relevé que les opérations litigieuses s'étaient, pour la plupart, succédées à environ une minute d'intervalle, ce qui rendait « peu vraisemblable » l'utilisation par le fraudeur de l'ensemble des codes des systèmes de sécurité de PAYWEB, « puisqu'il aurait fallu, en une minute environ, qu'il saisisse l'ensemble des données de confidentialité avant : d'opérer un autre achat en ligne dans la foulée, ce qui semble matériellement impossible » (jugement du 4 juillet 2014, p. 4, 3ème §) ; que pour contester ce motif, la Caisse de Crédit Mutuel de LILLE HELLEMES versait aux débats un constat d'huissier établi le 8 décembre 2014 attestant du processus hautement sécurisé du système mis en place par le Crédit Mutuel et que la durée de création d'une carte payweb telle que celle utilisée pour effectuer les débits litigieux n'était que de 21 secondes ; qu'en s'abstenant d'examiner, fût-ce de manière sommaire, le constat d'huissier produit par l'exposante qui démontrait le caractère erroné du motif retenu par le tribunal d'instance pour condamner l'exposante, la Cour d'appel a violé l'article 455 du code de procédure civile.

Décision attaquée : Cour d'appel de Douai , du 3 septembre 2015