



### **INFORMATION relative au rapport du conseiller rapporteur**

*Le présent rapport a été établi par un magistrat de la Cour de cassation, désigné conseiller rapporteur, en vue d'instruire une affaire (le « pourvoi en cassation ») soumise à la Cour de cassation. Au vu de ce rapport et des autres documents de la procédure, la Cour de cassation a tranché l'affaire par un arrêt, également diffusé sur Judilibre.*

*Ce rapport est un document de travail préparatoire établi, d'abord, à l'intention des magistrats du siège de la Cour appelés à trancher l'affaire. Ces magistrats sont des spécialistes de la question de droit examinée dans le rapport, qui n'a dès lors pas vocation à faire une présentation doctrinale de l'état du droit, mais à procéder à l'analyse de la procédure, des éléments de droit pertinents et des éventuels enjeux juridiques de l'affaire. Conformément au principe du contradictoire, ce document est également communiqué aux parties ou à leurs avocats, ainsi qu'à l'avocat général.*

*Enfin, ce rapport fournit une analyse à l'issue de laquelle le conseiller rapporteur ne donne pas son avis, lequel est soumis au secret du délibéré. Le rapport est donc toujours complété par deux autres documents établis par le rapporteur à l'intention des autres magistrats de la formation de jugement : une note d'avis et le ou les projets d'arrêts qu'il a préparés. Ces documents ne sont pas accessibles sur Judilibre.*

|                                                                              |    |
|------------------------------------------------------------------------------|----|
| N° N2419588                                                                  | C1 |
| <u>Décision attaquée</u> : 18 juin 2024, le tribunal de proximité de Morlaix |    |

|                             |  |
|-----------------------------|--|
| la société Banque CIC Ouest |  |
| C/                          |  |
| M. [T] [V]                  |  |
|                             |  |

Rapporteur : Valérie Champ

**RAPPORT en vue d'un rejet NON SPÉCIALEMENT  
MOTIVÉ du POURVOI - moyen(s) manifestement pas de  
nature à entraîner la cassation**

Il n'y a pas lieu de statuer par une décision spécialement motivée sur le pourvoi car les moyens qu'il invoque ne sont manifestement pas de nature à entraîner la cassation.

La Cour de cassation a, tout d'abord, jugé 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 ( [Com., 18 janvier 2017, pourvoi n° 15-18.102, Bull. 2017, IV, n° 6](#) ; [Com., 28 mars 2018, pourvoi n° 16-20.018, Bull. 2018, IV, n° 34](#)).

Elle a précisé la notion de négligence grave et retenu la preuve d'un tel manquement dans les cas suivants :

[Com, 25 octobre 2017, pourvoi n° 16-11.644, publié](#) :

« Prive sa décision de base légale, au regard des articles L. 133-16 et L. 133-19 du code monétaire et financier, la juridiction de proximité qui, pour condamner une banque à rembourser une somme prélevée sur le compte de son client au titre d'un paiement effectué par internet sans son autorisation, retient que ce dernier a communiqué, certes volontairement mais à la suite d'un hameçonnage, à une personne se présentant sous une fausse identité, les informations relatives à sa carte de paiement, qui ont ainsi été détournées à son insu, sans toutefois divulguer le code confidentiel de la carte, ni le code 3D Secure, de sorte qu'il ne peut lui être reproché de ne pas avoir respecté les dispositions de l'article L. 133-16 du code monétaire et financier, sans rechercher, au regard des circonstances de l'espèce, si ce client n'aurait pas pu avoir conscience que le courriel, auquel il avait ainsi répondu, était frauduleux et si, en conséquence, le fait d'avoir communiqué son nom, le numéro de sa carte de paiement, la date d'expiration de celle-ci et le cryptogramme figurant à son verso, ainsi que des informations relatives à son compte auprès de son opérateur téléphonique permettant à un tiers de prendre connaissance du code 3D Secure, ne caractérisait pas un manquement, par négligence grave, à ses obligations mentionnées à l'article précité. (Sommaire) »

[Com., 28 mars 2018, pourvoi n° 16-20.018, Bull. 2018, IV, n° 34](#) :

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

Attendu que pour statuer comme il fait, l'arrêt, après avoir relevé que M. [K] a été victime d'un hameçonnage, ayant reçu des courriels successifs portant le logo parfaitement imité du Crédit mutuel accompagnés d'un "certificat de sécurité à remplir attentivement" qu'il a scrupuleusement renseignés, allant même jusqu'à demander à la banque la communication de sa nouvelle carte de clés personnelle pour pouvoir renseigner complètement le certificat litigieux, ce qui montre sa totale naïveté, retient que la banque convient que seul un

examen vigilant des adresses internet changeantes du correspondant ou certains indices, comme les fautes d'orthographe du message, sont de nature à interpeller le client, ce à quoi n'est pas nécessairement sensible un client non avisé, étant observé que M. [K], qui ne se connectait quasiment jamais au site internet de la banque, ignorait les alertes de cette dernière sur le hameçonnage, puis en déduit que c'est à son insu que M. [K] a fourni les renseignements qui ont permis les opérations frauduleuses sur son compte et que n'est pas constitutive d'une négligence grave le fait pour un client "normalement" attentif de n'avoir pas perçu les indices propres à faire douter de la provenance des messages reçus ;

Qu'en statuant ainsi, 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 attentif de douter de sa provenance , peu important qu'il soit, ou non, avisé des risques d'hameçonnage, la cour d'appel a violé les textes susvisés. »

[Com, 6 juin 2018, pourvoi n° 16.029.065, inédit](#) :

« 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 ;

Attendu, selon l'arrêt attaqué, que Mme [Q], titulaire d'un compte dans les livres de la Caisse de crédit mutuel de [Localité 1](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 [Q] l'a assignée en paiement ;

Attendu que pour condamner la Caisse à rembourser à Mme [Q] 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 ;

Qu'en statuant ainsi, après avoir relevé que Mme [Q] 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. »

Elle a, en outre, écarté l'argument tiré de la bonne foi du client victime de la fraude pour écarter, ne serait-ce que partiellement, sa responsabilité ( [Com, 1<sup>er</sup> juillet 2020, 18-21.487, publié](#) ).

La Cour de cassation a, en revanche, récemment jugé qu'aucune négligence grave au sens de l'article L. 133-19 du CMF ne peut être imputée au titulaire d'un compte qui, contacté téléphoniquement par une personne se faisant passer pour un préposé de sa banque dont le numéro s'affichait , utilise à sa demande le dispositif de sécurité personnalisé pour supprimer puis réinscrire des bénéficiaires de virements dans le but

d'éviter des opérations malveillantes ( [Com., 23 octobre 2024, pourvoi n° 23-16.267, publié](#) )

On rappellera également que si la preuve d'un manquement par négligence grave du client a semblé suffisant dans un premier temps pour mettre à sa charge l'ensemble des conséquences financières des opérations réalisées frauduleusement avant qu'il ne forme opposition, la Cour de cassation a, dans un second temps, précisé qu'il résulte des articles L. 133-19, IV, et L. 133-23 du code monétaire et financier, dans leur rédaction issue de l'ordonnance n° 2009-866 du 15 juillet 2009, que s'il entend faire supporter à l'utilisateur d'un instrument de paiement doté d'un dispositif de sécurité personnalisé les pertes occasionnées par une opération de paiement non autorisée rendue possible par un manquement de cet utilisateur, intentionnel ou par négligence grave, aux obligations mentionnées aux articles L. 133-16 et L. 133-17 de ce code, le prestataire de services de paiement doit aussi prouver que l'opération en cause a été authentifiée, dûment enregistrée et comptabilisée et qu'elle n'a pas été affectée par une déficience technique ou autre ( [Com., 12 novembre 2020, pourvoi n° 19-12.112, publié](#) ). Cette solution rendue en application de la DSP1 a, par suite, été réitérée en application de la DSP2 ( [Com., 20 novembre 2024, pourvoi n° 23-15.099, publié](#) ; ; [Com., 30 avril 2025, pourvoi n° 24-10.149, publié](#) ).

Elle juge enfin de manière constante 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 ( [Com., 27 mars 2024, pourvoi n° 22-21.200, publié](#) ; [Com., 15 janvier 2025, pourvoi n° 23-13.579, publié](#) ). Elle admet inversement l'application d'un régime de droit commun, dès lors qu'une opération autorisée est en cause ( [Com., 2 mai 2024, pourvoi n° 22-17.233, publié](#) ).

Ayant exactement relevé que l'utilisateur avait été sollicité via le numéro officiel de son agence bancaire, pendant les horaires d'ouverture, que ces circonstances étaient de nature à le convaincre de la légitimité de son interlocuteur et que la banque n'explicitait pas le fait que le numéro officiel de l'agence ait pu être utilisé, le tribunal, qui n'était pas tenu de procéder à la recherche prétendument omise visée par le *troisième moyen*, a pu en déduire, indépendamment des motifs erronés mais surabondants critiqués par le *premier moyen*, que l'utilisateur n'avait pas commis de négligence grave et que la banque devait être condamnée au paiement ( ***réponse au deuxième moyen*** ).

#### **Demandes formées au titre de l'article 700 du CPC :**

|                                                 |                                                                                        |
|-------------------------------------------------|----------------------------------------------------------------------------------------|
| Mémoire ampliatif (la société Banque CIC Ouest) | Déposé le 30 décembre 2024<br>Signifié le 24 janvier 2025<br>Article 700 : 4 000 euros |
| Pas de constitution en défense                  |                                                                                        |

Il est proposé de rejeter la demande de la société Banque CIC Ouest.