REPUBLIQUE FRANCAISE
AU NOM DU PEUPLE FRANCAIS

Cour d'appel d'Orléans
CHAMBRE COMMERCIALE, ÉCONOMIQUE ET FINANCIÈRE
ARRÊT DU 04 AVRIL 2019

N° de RG: 18/008261

Infirme partiellement, réforme ou modifie certaines dispositions de la décision déférée

DÉCISION ENTREPRISE : Jugement du Tribunal de Commerce de TOURS en date du 08 Décembre 2017

PARTIES EN CAUSE

APPELANTE :- Timbre fiscal dématérialisé No: 1265223659547405
BANQUE POPULAIRE VAL DE FRANCE
agissant poursuites et diligences de son représentant légal domicilié en cette qualité audit siège [...]

Ayant pour avocat postulant Me Valerie DESPLANQUES de la SCP VALERIE DESPLANQUES, avocat au barreau d'ORLEANS, et pour avocat plaidant Me Eric NEGRE, membre de la SCP SAINT-CRICQ, NEGRE ET LA RUFFIE, avocat au barreau de TOURS,

D'UNE PART

INTIMÉE : - Timbre fiscal dématérialisé No: 1265222928524850
SARL ACTIMECA-C...
prise en la personne de son gérant domicilié en cette qualité audit siège [...]

Ayant pour avocat postulant Me Olivier LAVAL, membre de la SCP LAVAL - FIRKOWSKI, avocat au barreau d'ORLEANS, et pour avocat plaidant Me Sandrine BEAUGE GIBIER, membre de la SELAS FIDAL, avocat au barreau de CHARTRES,

D'AUTRE PART

DÉCLARATION D'APPEL en date du : 19 Mars 2018
ORDONNANCE DE CLÔTURE du : 22 novembre 2018 2019

COMPOSITION DE LA COUR

Lors des débats à l'audience publique du 24 JANVIER 2019, à 14 heures, Madame Elisabeth HOURS, Conseiller présidant la collégialité, en son rapport, et Monsieur Jean-Louis BERSCH, Conseiller, ont entendu les avocats des parties en leurs plaidoiries, avec leur accord, par application de l'article 786 et 907 du code de procédure civile.

Après délibéré au cours duquel Madame Elisabeth HOURS, Conseiller présidant la collégialité, et Monsieur Jean-Louis BERSCH, Conseiller, ont rendu compte à la collégialité des débats à la Cour composée de :

Madame Elisabeth HOURS, Conseiller présidant la collégialité,
Monsieur Jean-Louis BERSCH, Conseiller,
Madame Fabienne RENAULT-MALIGNAC, Conseiller,

Greffier :
Madame Marie-Lyne EL BOUDALI, Greffier lors des débats,
Madame Marie-Claude DONNAT, Greffier lors du prononcé,

ARRÊT :

Prononcé le 04 AVRIL 2019 par mise à la disposition des parties au Greffe de la Cour, les parties en ayant été préalablement avisées dans les conditions prévues au deuxième alinéa de l'article 450 du code de procédure civile.

EXPOSÉ DU LITIGE :

La société ACTIMECA-C..., qui a ouvert un compte dans les livres de la Banque Populaire Val de France (la BPVF), a constaté le 17 août 2015 le virement frauduleux d'une somme de 94.752,90 euros au profit de Monsieur Z... I....

Après avoir déposé plainte, elle a sollicité le remboursement de cette somme par la banque, laquelle a refusé en faisant valoir que la fraude n'avait pu être commise qu'en raison de l'imprudence d'ACTIMECA-C... qui avait laissé en permanence branchée sur son ordinateur la clef Certeurope lui permettant de procéder à ses transactions bancaires par Internet.

Le 24 mai 2016, ACTIMECA-C... a en conséquence assigné la BPVF devant le tribunal de commerce de Tours en réclamant restitution de la somme frauduleusement débitée de son compte outre versement de dommages et intérêts et d'une indemnité de procédure.

Par jugement en date du 8 décembre 2017, le tribunal a condamné la BPVF à rembourser la somme de 94.752,90 euros et alloué à la demanderesse, qu'il a déboutée du surplus de ses demandes, 8.440,38 euros en réparation de son préjudice financier et 7.000 euros sur le fondement de l'article 700 du code de procédure civile.

La BPVF a relevé appel de cette décision par déclaration en date du 19 mars 2018.
Elle en poursuit l'infirmation, hormis en ce qu'elle a débouté ACTIMECA-C... de sa demande d'indemnisation d'un préjudice moral, en demandant à la cour de débouter l'intimée de toutes ses demandes et de la condamner à lui verser une indemnité de procédure de 6.000 euros ainsi qu'à supporter les dépens dont distraction au profit de Maître DESPLANQUES.

Elle demande à la cour d'écarter le rapport établi non contradictoirement par la société Expertis qui conclut que l'intrusion malveillante dans le système informatique découle de

l'infection par le malware DRIDEX, d'un défaut de vigilance d'ACTIMECA-C... entre le 7 et le 17 août 2015, d'une insuffisance des précautions du dispositif CYBERPLUS de la BPVF, d'un défaut de surveillance et de contrôle des clients CYBERPLUS par la banque, d'un défaut de détection du caractère atypique du virement par l'agence BPVF, d'un défaut d'alerte et de mise en garde contre les risques encourus lors de l'utilisation de la clé de sécurité et de CYBERPLUS alors qu'il existait un risque caractérisé de propagation du malware durant l'été 2015.

Elle fait valoir que c'est en inversant la charge de la preuve que les premiers juges ont retenu qu'elle ne démontrait ni que la clef Certeurope avait été laissée sur l'ordinateur d'ACTIMECA-C... ni que celle-ci ne changeait pas assez souvent son code PIN.

Elle fait valoir qu'ACTIMECA-C... a nécessairement été victime d'un hameçonnage et a ouvert un courriel frauduleux qui a permis la contamination de son système informatique, laquelle résulte en conséquence d'une succession de manoeuvres fautives de l'intimée.

Elle rappelle qu'aux termes de l'article L.133-16 du code monétaire et financier, l'utilisateur de services de paiement prend toute mesure raisonnable pour préserver la sécurité des dispositifs de paiement qu'il reçoit ; qu'ACTIMECA-C... A ne démontre pas avoir choisi et acquis un antivirus adapté et produit une facture qui ne précise pas le matériel acquis et que cet achat démontre qu'en tout état de cause elle a été sans protection antivirus entre le 15 mai 2014 et le 10 mars 2015. Elle souligne que l'article 4 du contrat d'abonnement produit par l'intimée elle-même prévoit au paragraphe UTILISATION DU SERVICE : «s 'agissant des opérations effectuées par le canal Internet, il est rappelé qu'en dépit de toutes les précautions prises par la Banque, l'espace Internet demeure un espace non régulé dont l 'utilisation présente des risques nombreux. Il appartient au porteur (de la clé) sous sa responsabilité de protéger son matériel informatique en adoptant la solution de sécurité (firewall et anti-virus notamment) de son choix.››. Et elle souligne qu'ACTIMECA-C... est assistée d'un infogérant informatique, la société FEPP à laquelle elle a confié l'externalisation de tout ou partie de la gestion et de l'exploitation de son service informatique ; que l'étude commandée par l'intimée démontre que la fraude a eu lieu ensuite de la contamination par le virus DRIDEX via un fichier word reçu le 15 juillet 2015 soit plus de trois semaines avant le virement frauduleux ; que la lecture du message ayant engendré la contamination permet de vérifier que non seulement il provenait d'un émetteur inconnu d'ACTIMECA-C... mais que celui-ci avait utilisé l'adresse : gerardHicksj\w@venusinblue.com, qui aurait d'autant plus dû éveiller la méfiance de l'intimée que l'objet du message était une demande en paiement de facture qui ne pouvait avoir été émise par cet interlocuteur ; qu'il existait donc des indices permettant à un utilisateur normalement attentif de douter de la provenance de ce message ; que ces indices n'ont pas empêché ACTIMECA-C... d'ouvrir non seulement le mail mais également le fichier joint ; qu'elle a nécessairement activé les macros après avoir trouvé un fichier vierge et que ce sont ces trois fautes successives qui ont permis l'entrée du virus dans son système informatique.

Elle prétend par ailleurs que l'infection par un «macro virus›› entraîne des dysfonctionnements de l'ordinateur tel qu'un ralentissement ou des demandes inhabituelles comme un mot de passe pour un fichier qui n'en requiert normalement pas, ou autres anomalies qui auraient dû conduire ACTIMECA-C... à réagir devant ces alertes qui sont passées sous silence par le cabinet Expertis.

Elle souligne qu'en application de l'article L.133-19 du code monétaire et financier le payeur supporte toutes les pertes occasionnées par des opérations de paiement non autorisées lorsqu'il n'a pas satisfait intentionnellement ou par négligence grave aux obligations mentionnées aux articles L 133-16 et L 133-17 ; que les obligations d'ACTIMECA-C... lui étaient rappelées par l'article 10 des conditions générales qui précisaient qu'elle devait :
- Protéger son module cryptographique contre toutes détériorations physiques et le garder sous son contrôle exclusif de toutes circonstances
- Modifier régulièrement son code PIN et le protéger de toute compromissions par perte, vol ou capture informatiques - Assurer la sécurité du poste informatique sur lequel il utilise le certificat électronique
- Fermer son navigateur ou toute application nécessitant l'utilisation de son module cryptographique après utilisation
- Débrancher son module cryptographique après toute utilisation.

Elle affirme qu'il résulte tant du dépôt de plainte d'ACTIMECA-C... que de son courriel en date du 17 août 2015 que l'intimée n'avait pas retiré la clef de l'ordinateur, ce qui constitue une négligence grave et qu'il ressort d'ailleurs de l'étude réalisée à la demande de l'intimée qu'un piratage ne peut intervenir que lorsque la clef est branchée.

Elle reproche également à la gérante d'ACTIMECA-C... , qui est venue travailler le 10 août sur la comptabilité, de ne pas avoir détecté le virement opéré le 7 août, ce qui a empêché la banque de mettre en place en urgence la procédure de retour du virement auprès de la banque bénéficiaire.

Elle soutient que la sécurité du système CYBERPLUS ne saurait être remise en cause puisque ce n'est pas ce système qui a été touché par le virus, mais bien le système informatique d'ACTIMECA-C....

Elle fait valoir que le tribunal s'est fourvoyé en lui reprochant de ne pas avoir produit le RIB ainsi que l'ordre de virement qu'elle a reçu de l'escroc puisqu'il s'agissait d'un virement par Internet, nécessairement sans RIB et sans bordereau papier.

A titre infiniment subsidiaire, elle conteste que l'intimée ait subi un préjudice économique et fait valoir qu'elle a procédé à des rétrocessions de frais, a pris en charge des commissions d'intervention sur les mois d'août et de septembre 2015, et a accordé à ACTIMECA-C... un prêt d'un montant de 98.000 euros le 10 septembre 2015 pour une durée de 84 mois au taux de 1,8%. Elle affirme par ailleurs que l'intimée ne saurait, au regard de ses imprudences et négligences, solliciter l'indemnisation d'un préjudice moral.

ACTIMECA-C... conclut à la confirmation du jugement déféré, hormis en ce qu'il a refusé de faire droit à ses demandes tendant au paiement de 4.175,52 euros au titre des frais d'audit, ainsi que de 5.000 euros à titre de dommages et intérêts en réparation de son préjudice moral et elle demande à la cour de lui allouer ces sommes ainsi qu'à lui verser une nouvelle indemnité de procédure de 3.500 euros et à supporter les dépens.

Elle rappelle que la banque, en sa qualité de professionnelle, a l'obligation de restituer les fonds lorsque le virement est frauduleux et ne peut s'exonérer de cette obligation que par la démonstration d'une faute grave du titulaire du compte. Elle fait valoir qu'elle produit la facture ainsi que le bon de livraison de son prestataire informatique, qui démontrent l'installation d'un équipement anti virus en mars 2015, pour une version parfaitement actualisée et ce pour 2 ans. Elle rappelle que la cyber-attaque DRIDEX, survenue en juin/juillet 2015 à un niveau national, n'était pas arrêtée par les outils de l'époque. Elle prétend que le fait qu'elle ait été assistée par un gestionnaire informatique n'est pas de nature à exonérer l'appelante de ses propres obligations. Et elle souligne que le virement litigieux a été effectué en août 2015 durant la période de congés ; que, si Madame C..., qui s'occupe de la comptabilité, est venue travailler et a effectué des opérations informatiques le 10 août 2015 dans les locaux de la société, ces opérations n'ont concerné que les salaires et les opérations de gestion pour l'entreprise et qu'il ne peut lui être reproché un manque de surveillance de ses comptes puisque l'opération bancaire de virement n'apparaissait pas à cette date. Elle affirme que le message de hameçonnage ne pouvait l'alerter puisqu'il ne contient pas d'indices particuliers de malveillance pour un utilisateur normalement attentif et ne comporte notamment pas de fautes d'orthographe et elle souligne qu'elle n'y a pas répondu.

Elle fait valoir que l'appelante ne démontre aucunement sa négligence dans l'utilisation de la clef ; que la BPVF s'est empressée d'interroger Madame C... par téléphone pour savoir si la « clé de sécurité » était installée sur l'ordinateur et de l'inviter à l'écrire par mail ; qu'il suffit de lire le mail de réponse de Madame C... pour constater que la phrase liée à la présence de la clé sur l'ordinateur n'a pas la portée que la BANQUE POPULAIRE lui donne puisque Madame C... parle du 10 août 2015, date à laquelle elle est venue travailler et non de la période antérieure ; qu'il ne peut être tiré de ce courriel la démonstration que la clé Certeurope est restée branchée en permanence. Et elle affirme qu'en tout état de cause un tel branchement permanent ne serait pas déterminant de l'escroquerie puisqu'il résulte du rapport Expertis qu'il suffit que la clé soit insérée un instant, une fois le logiciel malveillant installé, pour que celui-ci profite du moment de l'utilisation de la clé et de la saisie complémentaire du code PIN, pour détourner les informations et créer un faux ordre de virement.

Elle souligne que l'article 10 des conditions particulières du contrat sur lequel la BPVF fonde son argumentation d'une parfaite information des dangers encourus fait état de différentes obligations, dont celle de "débrancher son module cryptographique", ce qui manque pour le moins de clarté ; qu'elle fait référence soit à la « clé privée » soit au « certificat numérique» ou encore au « module cryptographique » ; qu'au surplus, le contrat et les conditions générales et particulières laissent penser que la clé est un outil de sécurité, ce qui n'était pas le cas. Et elle précise qu'en ce qui concerne les fraudes susceptibles d'intervenir sur le site CYBERPLUS, la BPVF préconise des règles de prudence sans jamais mentionner d'avoir à déconnecter la clef. Elle reproche à l'appelante de ne pas avoir spécifiquement ses clients de la dangerosité du virus DRIDEX qu'elle ne pouvait ignorer.

Elle fait valoir que, si elle procédait à des virements régulièrement, ceux-ci ne dépassaient jamais 6.000 euros, hormis pour des paiements de ses salariés, ce qui aurait dû conduire la banque à s'étonner d'un virement de 94.752, 90 euros à destination d'un pays étranger intervenu en plein mois d'août sans courriel d'accompagnement contrairement à ses habitudes.

Elle insiste sur le fait que les documents produits par l'appelante indiquent qu'il appartient à la banque de vérifier si l'ordre est valide et exécutable à la charge du donneur d'ordre et demande à la cour de constater les manquements de l'appelante à ses obligations et à tout le moins de retenir que n'est établi aucun manquement grave à celles qui lui incombaient en qualité de titulaire du compte. Et elle souligne qu'elle a produit le rapport de la société Expertis, non comme un rapport d'expertise, mais comme un avis lui permettant de combattre les affirmations de la BPVF d'une mauvaise utilisation de la clef de paiement.

CELA ETANT EXPOSE, LA COUR :

Attendu que l'article L.133-23 du code monétaire et financier énonce que« lorsqu'un utilisateur de services de paiement nie avoir autorisé une opération de paiement qui a été exécutée, ou affirme que l'opération de paiement n'a pas été exécutée correctement, il incombe à son prestataire de services de paiement de prouver que l'opération en question a été authentifiée, dûment enregistrée et comptabilisée et qu'elle n'a pas été affectée par une déficience technique ou autre. L'utilisation de l'instrument de paiement telle qu'enregistrée par le prestataire de services de paiement ne suffit pas nécessairement en tant que telle à prouver que l'opération a été autorisée par le payeur ou que celui-ci n'a pas satisfait intentionnellement ou par négligence grave aux obligations lui incombant en la matière » ;

Que l'article L.133-18 du même code précise qu'« 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 » ;

Qu'il résulte de ces dispositions que pèse sur la banque la charge de la preuve d'une négligence grave de son client ayant entraîné l'utilisation frauduleuse de ses moyens de paiement ;

Qu'il convient dès lors, avant même de rechercher si la banque a elle-même commis un manquement à ses obligations contractuelles, de vérifier sir ACTIMECA- C... s'est montrée gravement négligente ;

Attendu qu'en l'espèce, la BPVF prétend que la société ACTIMECA-C... se serait montrée imprudente d'une part en ne s'équipant pas d'un anti virus, d'autre part en ouvrant une pièce jointe à un mail ne pouvant émaner de l'un de ses clients ou fournisseurs, enfin en laissant branchée en permanence la clef Certeurope permettant les transactions par Internet ;

Que, pour démontrer le contraire, l'intimée produit le rapport établi à sa demande par la société Expertis qu'elle a mandatée pour rechercher les causes du piratage ;

Que ce rapport n'est aucunement un rapport d'expertise fondant les demandes d'ACTIMECA-C... mais un rapport d'une société spécialisée visant à déterminer les circonstances du virement frauduleux et les causes ayant pu le permettre ;

Qu'il répond uniquement aux dires de la BPVF d'une négligence grave commise par sa cliente et est en conséquence un avis technique pouvant être combattu par un autre avis technique ;

Que, non seulement la banque ne communique ni expertise ni avis technique, alors même qu'il résulte de ses propres pièces que le sinistre subi par ACTIMECA-C... est un sinistre sériel puisque de très nombreuses sociétés ont connu le même piratage, mais qu'elle utilise à plusieurs reprises le rapport Expertis qu'elle cite quand il peut lui être favorable tout en demandant à la cour de l'écarter ;

Attendu que contrairement à ce que prétend la BPVF, ACTIMECA-C... démontre qu'elle avait acquis, en mars 2015, un anti virus efficace et suffisant au regard des antivirus alors sur le marché ;

Que c'est sans pertinence que la banque soutient que la protection du système informatique n'est pas établie avant cette date puisque d'une part, il résulte des pièces communiquées par l'intimée qu'il s'agissait pour elle en mars 2015 de renouveler sa protection antivirus existante et que d'autre part la BPVF reconnaît elle-même que l'attaque a débuté le 7 août 2015 seulement et qu'une absence de protection antérieure à cette date aurait donc été indifférente ;

Attendu ensuite qu'il résulte de l'analyse Expertis que le système informatique d'ACTIMECA -C... a été infesté par le virus DRIDEX, ce qui n'est pas contesté par l'appelante ;

Que la BPVF produit elle-même, sous le numéro 16 de ses pièces communiquées, un avis d'alerte en date du mois de juin 2015 émanant du Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques qui indique que le CERT-FR constate à l'échelle nationale une vague de pourriels dont le taux de blocage par les passerelles anti-pourriel est relativement faible ; que ces pourriels, très souvent rédigés dans un français sans faute, font état de problèmes de facturation, dans la plupart des cas, pour inciter la victime à ouvrir la pièce jointe ;

Qu'elle communique divers documents sous ses pièces 17,18 et 19 qui démontrent que dès juin 2015, les banques étaient informées des attaques du virus DRIDEX affectant principalement les transactions bancaires par Internet ;

Que toujours dès juin 2015, elles étaient avisées que le malware DRIDEX permettait de procéder à des versements bancaires frauduleux portant sur plusieurs millions d'euros, les articles communiqués par l'appelante elle-même faisant état d'une "attaque de forte ampleur" ;

Que les conseils donnés dès juin 2015 par ces articles, qui constataient unanimement le peu d'efficacité des antivirus pour parer aux attaques de DRIDEX puisque seuls de rares anti-malware permettaient de détecter les documents les contenant, étaient de désactiver l'exécution automatique des macros dans les sites bureautiques ;

Que, parfaitement informée des risques encourus par ses clients, la BPVF ne les en a cependant pas alertés et n'a pas donné le conseil de désactivation de l'exécution automatique des macros ;

Qu'elle ne saurait donc sérieusement soutenir qu'ACTIMECA-C..., non avisée de cette attaque, aurait commis une négligence grave en ouvrant la pièce jointe à un message rédigé en français parfait et sans fautes d'orthographe qui faisait état d'une difficulté de facturation, l'intimée ne pouvant en effet raisonnablement penser qu'il s'agissait d'un spam ;

Que l'ouverture du fichier joint à un tel message n'était dès lors pas imprudente en l'absence d'information donnée par la banque sur la méthode employée pour infester le système de la société et que c'est l'ouverture non fautive de la pièce jointe au message malveillant qui a permis l'entrée du virus dans le système d'ACTIMECA-C... ;

Qu'il n'est en effet pas contesté que l'ouverture de la pièce jointe au message reçu le 7 août 2015 a permis, le 10 août 2015, l'ajout frauduleux d'un nouveau RIB à la liste des destinataires des virements autorisés dans la base d'information de CYBERPLUS relative au compte ACTIMECA -C... et que c'est ce compte frauduleux qui a été utilisé pour effectuer le virement ;

Que l'appelante qui procède par affirmations sans aucun avis technique permettant d'appuyer ses dires ne justifie aucunement que le virus DRIDEX entraînait des dysfonctionnements du système informatique qui auraient dû alerter ACTIMECA-C... et n'expose pas en quoi l'assistance d'un infogérant informatique aurait permis à l'intimée de détecter ce virus ;

Attendu enfin, que la BPVF entend démontrer le maintien de la clef en permanence sur l'ordinateur la production d'un mail adressé le 17 août 2015 par Madame C... en ces termes : "Je vous confirme qu'un virement frauduleux d'un montant de 94.752,90 euros a été effectué sur le compte no [...] le 10/08/15 au bénéfice de Z... I.... La clé du système transfert sécurisé était installée sur l'ordinateur. Nous comptons sur vos services pour remonter la filière de cette fraude".

Que, contrairement à ce que soutient l'appelante, il ne peut être établi par ce courriel que la clé Certeurope était laissée en permanence par Madame C... sur l'ordinateur de la société ;

Qu'en effet, Madame C... est venue travailler le 10 août 2015, jour de la réalisation du virement frauduleux, et qu'il n'est pas justifié qu'elle n'était pas présente et n'utilisait pas normalement la clef Certeurope au moment où le virement frauduleux a été réalisé ;

Que la preuve d'un maintien constant de la clef sur l'ordinateur ne résulte pas plus du dépôt de plainte déposé par la société puisque son dirigeant a déclaré aux enquêteurs : "Nous utilisons un système évolué de cryptage des données avec en sus l'obligation de la présence physique d'une clef USB en déverrouillage laquelle était très probablement présente encore sur l'ordinateur. Un nouveau RIB client a été créé le 7 août 2015 et ajouté à notre base. C'est avec ce RIB que la transaction a été réalisée" ;

Qu'il n'a donc pas été reconnu, contrairement à ce que prétend la BPVF, que la clef demeurait en permanence sur l'ordinateur de la société mais simplement qu'elle y était "probablement encore" lorsque le virement a été réalisé ;

Qu'en tout état de cause, la société Expertis a souligné, dans son avis technique qui n'est démenti par aucun autre avis, que la connexion de la clé de sécurité n'est pas la cause du sinistre, les connexions et déconnexions de la clé pouvant éventuellement ralentir le processus de la fraude mais ne pouvant véritablement l'empêcher puisqu'il faut en tout état de cause la laisser connectée le temps suffisant à l'élaboration d'un virement ; que le fait qu'elle soit connectée 10 minutes, 1 heure ou une matinée est en conséquence indifférent dès lors que le système est infesté ;

Attendu qu'il résulte de ce qui vient d'être exposé que la BPVF échoue à rapporter la preuve qui lui incombe d'une faute ou d'une négligence grave commise par sa cliente ;

Qu'en application de l'article L.133-23 du code monétaire et financier, le jugement déféré sera donc confirmé en ce qu'il l'a condamnée à rembourser la somme détournée ;

Attendu que c'est sans sérieux que la BPVF prétend qu'ACTIMECA-C... n'aurait subi aucun préjudice financier puisqu'elle lui a consenti un prêt 98.000 euros le 10 septembre 2015 pour une durée de 84 mois au taux de 1,8% ;

Qu'en effet, l'intimée, qui aurait dû recevoir immédiatement remboursement, a vu sa trésorerie impactée par le remboursement de ce prêt qu'elle a été contrainte de souscrire en raison du refus fautif de sa banque de lui restituer les fonds détournés;

Que le jugement déféré sera également confirmé en ce qu'il a réparé ce préjudice par l'octroi de la somme de 8.440,38 euros à titre de dommages et intérêts ;

Et attendu que la société ACTIMECA-C..., cliente depuis trente années de la BPVF, a indiscutablement subi un préjudice moral résultant des soucis qui lui ont été causés par la situation difficile dans laquelle elle se trouvait et de l'obligation de rechercher en urgence des solutions de financement alors que sa situation de trésorerie était en péril et qu'elle pouvait craindre un état de cessation des paiements;

Que, par infirmation du jugement critiqué, ce préjudice sera réparé par l'octroi d'une somme de 2.000 euros ;

Attendu qu'ACTIMECA-C... reproche sans fondement au tribunal d'avoir rejeté sa demande tendant au paiement de la somme de 4.175,52 euros engagée au titre des frais d'audit du système informatique ;

Qu'en effet, ces frais, exposés pour se défendre de l'accusation de négligence formulée par la BPVF, entrent dans les dispositions de l'article 700 du code de procédure civile et que le tribunal, en accordant de ce chef à ACTIMECA-C... une somme de 7.000 euros en a nécessairement tenu compte ;

Que le jugement déféré sera dès lors confirmé en ce qu'il a rejeté cette demande formée en sus de celle présentée au titre des frais irrépétibles ;

Attendu que la BPVF succombant en toutes ses prétentions supportera les dépens d'appel et qu'il sera fait application, au profit de l'intimée, des dispositions de l'article 700 du code de procédure civile ;

PAR CES MOTIFS

Statuant par arrêt mis à disposition au greffe, contradictoire et en dernier ressort,

CONFIRME la décision entreprise, hormis en ce qu'elle a rejeté la demande de la société ACTIMECA-C... tendant à l'indemnisation d'un préjudice moral,

STATUANT À NOUVEAU de ce seul chef,

CONDAMNE la Banque Populaire Val de France à payer à la société ACTIMECA-C... la somme de 2.000 euros en réparation de son préjudice moral,

Y AJOUTANT

CONDAMNE la Banque Populaire Val de France à payer à la société ACTIMECA-C... la somme de 2.000 euros au titre des dispositions de l'article 700 du code de procédure civile,

CONDAMNE la Banque Populaire Val de France aux dépens d'appel.

Arrêt signé par Madame Elisabeth HOURS, Conseiller présidant la collégialité, et Madame Marie-Claude DONNAT, Greffier auquel la minute de la décision a été remise par le magistrat signataire.

LE GREFFIER
LE PRÉSIDENT