



Copie exécutoire : [REDACTED]  
Copie aux demandeurs : 2  
Copie aux défendeurs : 2

REPUBLIQUE FRANCAISE

AU NOM DU PEUPLE FRANCAIS

TRIBUNAL DES ACTIVITES ECONOMIQUES DE PARIS

CHAMBRE 1-10

JUGEMENT PRONONCE LE 16/01/2026  
par sa mise à disposition au Greffe

RG 202 [REDACTED]

ENTRE :

[REDACTED] dont le siège social est [REDACTED]  
[REDACTED]

Partie demanderesse : assistée de Me Maude HUPIN Avocat (G0625) et comparant par [REDACTED]

ET :

SAS OLINDA, dont le siège social est 18 rue de Navarin 75009 Paris - RCS B 819489626

Partie défenderesse : assistée de la SELAS CLOIX & MENDES-GIL - Me Sébastien MENDES-GIL Avocat (P173) et comparant par le cabinet TREHET AVOCATS ASSOCIES AARPI – Me Virgine TREHET Avocat (J119)

APRÈS EN AVOIR DÉLIBÉRÉ

### LES FAITS – L’OBJET DU LITIGE

Le demandeur, la société [REDACTED], détient un compte bancaire professionnel auprès de la société OLINDA (ci-après la BANQUE), qui exerce sous le nom commercial Qonto. Ce compte est équipé d’une carte bancaire numéro \*\*\*\* [REDACTED]

Le 10 janvier 2024 vers 15h30, aux dires du CLIENT, il a été victime d’une fraude bancaire de type « *spoofing* », c’est à dire avec usurpation d’identité d’un conseiller bancaire, visant à lui faire croire qu’il était en ligne avec le service fraude de sa banque qui avait détecté des opérations frauduleuses. L’échange téléphonique a duré près d’une heure. Cette fraude a abouti à la réalisation de plusieurs opérations de paiement à distance par cartes bancaires pour une somme totale de 14.147,50 euros.

Le 15 janvier 2024, le CLIENT a déposé plainte.

Le CLIENT a immédiatement contesté ces opérations non sollicitées et non validées mais la BANQUE a refusé toute indemnisation.

C'est dans ces circonstances que le demandeur a engagé la présente instance.

### LA PROCÉDURE

Le CLIENT a fait assigner la BANQUE par acte remis le 16 avril 2024 à personne se déclarant habilitée à recevoir une copie.

En application des dispositions de l'article 446-2 du code de procédure civile, le tribunal retiendra les dernières conclusions récapitulatives de chacune des parties avec les dernières demandes formulées par écrit et communiquées par elles.

Par ses conclusions régularisées à l'audience du 27 novembre 2025, le CLIENT demande au tribunal de :

*Vu les articles L133-6 et suivants du Code monétaire et financier,*

*Vu l'article 1343-2 du Code civil,*

- DECLARER la société [REDACTED] bien fondée en ses demandes, fins et conclusions,
- DEBOUTER la société OLINDA de l'ensemble de ses demandes, fins et prétentions,
- CONDAMNER la société OLINDA à payer à la société [REDACTED] la somme de 14.147,50 euros en remboursement des sommes détournées, outre les intérêts au taux légal majoré de quinze points,
- ORDONNER la capitalisation des intérêts,
- CONDAMNER la société OLINDA à payer à la société [REDACTED] la somme de 3.000 euros au titre de la résistance abusive,
- CONDAMNER la société OLINDA au paiement de la somme de 5.000 € au titre de l'article 700 du Code de procédure civile,
- CONDAMNER la société OLINDA aux entiers dépens,
- ORDONNER l'exécution provisoire

Par ses conclusions récapitulatives en défense soutenues à l'audience du 13 mars 2025, la BANQUE demande au tribunal de :

*Vu les pièces versées aux débats,*

*Vu les articles L. 133-1 et suivants du Code Monétaire et Financier,*

*Vu les articles L. 133-18, L. 133-19, L. 133-16 et L. 133-17 du Code Monétaire et Financier,*

*Vu la jurisprudence citée,*

- DECLARER la société OLINDA recevable et bien fondée en ses prétentions ;  
En conséquence,  
1. A TITRE PRINCIPAL :
  - DIRE et JUGER que les opérations litigieuses du 10 janvier 2024 sont des opérations de paiement autorisées et que la SAS THE [REDACTED] ne peut se prévaloir de l'article L. 133-18 du Code Monétaire et Financier ;
  - à tout le moins, DIRE ET JUGER que ces opérations ont été dûment enregistrées et comptabilisées au moyen d'un dispositif d'authentification forte, et n'ont pas été affectées par une déficience technique ;
  - en conséquence, DEBOUTER la SAS THE [REDACTED] de sa demande visant à voir la société OLINDA condamnée à lui verser la somme de 14.147,50 euros avec intérêts légaux majoré de quinze points et la somme de 3.000 euros au titre de la résistance abusive ;
- 2. A TITRE SUBSIDIAIRE :
  - DIRE et JUGER que la SAS THE [REDACTED] a commis une négligence grave en ne préservant pas la sécurité de ses données de sécurité personnalisées et en n'utilisant pas l'instrument de paiement mis à sa disposition conformément aux conditions qui régissent sa délivrance et son utilisation ;
  - en conséquence, DEBOUTER la SAS THE [REDACTED] de sa demande visant à voir la société OLINDA condamnée à lui verser la somme de 14.147,50 euros avec intérêts légaux au titre de son préjudice financier et la somme de 3.000 euros au titre de son préjudice moral ;
- 3. EN TOUT ETAT DE CAUSE
  - DEBOUTER la SAS THE [REDACTED] de l'intégralité de ses demandes, fins et conclusions ;

- CONDAMNER la SAS [REDACTED] à verser à la société OLINDA la somme de 3.500 euros au titre de l'article 700 du Code de procédure civile ;
- CONDAMNER la SAS [REDACTED] à supporter la charge des entiers dépens.

Ces demandes ont fait l'objet du dépôt de conclusions qui ont été échangées en présence d'un greffier qui les a visées sur la cote de procédure.

A son audience du 27 novembre 2025, le juge chargé d'instruire l'affaire a entendu les parties en leurs observations et explications, a clos les débats, a mis l'affaire en délibéré et a dit que le jugement sera prononcé par sa mise à disposition au greffe le 26 septembre 2025, date reportée au 16 janvier novembre 2025.

Par constat d'audience, le CLIENT précise demander la somme de 14.147,50 euros outre les intérêts au taux légal majoré de 15 points à compter du mois suivant la fraude, à savoir le 10 février 2024, et la somme de 3.000 euros à titre de préjudice moral.

### **MOYENS DES PARTIES**

Lorsque certains moyens et arguments n'auront pas été repris, il sera renvoyé aux écritures des parties et aux motifs de la décision, conformément aux dispositions de l'article 455 du code de procédure civile.

#### MOYENS DU DEMANDEUR

Le CLIENT, en demande, fait valoir que, en application des dispositions de l'article L. 133-18 du code monétaire et financier (ci-après CMF), le banquier ou le prestataire de services de paiement doit rembourser les opérations non autorisées par son client.

Et c'est à la banque de rapporter la preuve que son client, utilisateur de services de paiement, aurait agi frauduleusement ou n'aurait pas satisfait intentionnellement ou par négligence grave à ses obligations, au visa de l'article L. 133-23 du CMF.

Le CLIENT a été trompé, manipulé et a été victime d'une fraude non pas en raison de sa négligence grave, non caractérisée en l'espèce, mais en raison de la défaillance du système de la banque qui a connu à cette période de nombreuses fraudes bancaires sur lesquelles elle se garde bien de communiquer.

La version des faits de la BANQUE n'est confortée par aucune pièce, si ce n'est sa pièce n°1 qui est partiellement illisible et semble faire état de plusieurs adresses IP, ce qui confirme la réalité de la fraude.

Et le tribunal observera que toutes les autres pièces communiquées ne concernent pas le demandeur mais sont des pièces génériques.

De plus, aucune négligence ne peut lui être imputée dans la protection de ses données personnelles confidentielles. En effet le CLIENT ne pouvait aucunement savoir qu'un numéro de téléphone de sa banque pouvait ne pas être sécurisé et encore moins être usurpé par des fraudeurs pour se faire passer pour un service d'une banque. Ce qui est suffisant, comme l'a jugé récemment le Cour de cassation, à démontrer l'absence de négligence grave dans le cadre des manœuvres très sophistiquées utilisées par les fraudeurs, en ce que la technique d'arnaque avec usurpation d'un numéro de téléphone a mis en confiance le client et a réduit son niveau de vigilance.

Le CLIENT précise n'avoir jamais communiqué une information confidentielle mais avoir tout simplement saisi dans son application le code provisoire qui lui a été dicté par son interlocuteur : Il n'a donc pas été négligent en communiquant son code confidentiel.

C'est ainsi à tort que la BANQUE invoque la négligence grave de son client et prétend que la charge de la preuve repose sur le demandeur, par une combinaison et une interprétation personnelle des articles 1356 et 1358 du code civil. Ces moyens sont juridiquement erronés et reviendraient à contredire la règle « *selon laquelle la loi spéciale déroge sur la loi générale.* »

Enfin, le CLIENT a subi le refus injustifié de la BANQUE et demande la condamnation de la BANQUE à lui payer la somme de 3.000 euros au titre de la résistance abusive de cette dernière.

Il ne peut donc se voir opposer ni sa négligence grave, ni les dispositions générales contractuelles du compte bancaire qui renversent la charge de la preuve en cas de contestations d'opérations de paiement, en ce que le CLIENT n'a ni signées ni acceptées.

### MOYENS DU DEFENDEUR

A titre principal, le tribunal jugera que les ordres de paiement du CLIENT constituent des opérations autorisées protégées par un système d'authentification forte et que la demanderesse ne peut donc se prévaloir, de ce fait, de l'article L. 133-18 du CMF.

A tout le moins, il jugera que ces opérations ont été dûment enregistrées et comptabilisées au moyen d'un dispositif d'authentification forte, et n'ont pas été affectées par une déficience technique, conformément à l'article L. 133-23 du même code.

En l'espèce, la BANQUE produit le relevé des connexions (dits « logs techniques » ; pièce n°1) qui démontre que l'ensemble des opérations a été validé directement depuis l'appareil du CLIENT (iPhone 14 référencé 94d9e564-4374-4b3e-8727-87cc49dce7a5) : soit, au total, pas moins de 10 actions sensibles, poursuivant des finalités diverses, validées ainsi par le CLIENT. Ainsi ces logs techniques sont bien loin du récit partiel de la fraude dressé par le CLIENT, qui, loin de jouer un rôle passif, aura activement contribué à la réalisation du préjudice allégué.

Subsidiairement, la BANQUE oppose à son client qu'il a fait preuve de négligence grave dans la protection de ses données de sécurité personnalisées. En effet, si ces opérations ont pu être réalisées malgré le dispositif de sécurité avec authentification forte et si elles ne sont affectées d'aucune défaillance technique, il s'en déduit que soit elles ont été réalisées par le client, soit ce dernier a manqué à son obligation de protection de ses données de sécurité personnalisées.

La charge de la preuve de la négligence grave repose sur la BANQUE et, comme l'indique le demandeur, cette preuve ne peut pas se déduire du seul fait que l'instrument de paiement du client ou les données personnelles qui lui sont liées ont été utilisés pour la réalisation de l'opération contestée : autrement dit, la BANQUE doit prouver que le destinataire a confié - d'une manière ou d'une autre - ses données confidentielles au fraudeur. Or :

- d'une part, si le CLIENT reste taisant sur la divulgation ou non de ses données confidentielles (= le fait inconnu), le tribunal est parfaitement en droit d'en déduire qu'il les a communiquées au fraudeur à partir des éléments dont il dispose (les faits connus).
- d'autre part, les conditions générales de l'établissement peuvent librement aménager les modalités de preuve applicables entre les parties quand celles-ci sont commerçants. Or, l'article 3.3 du Titre II des conditions générales (Ci-après CG) de Qonto indique que « *si le paiement a été initié à la suite d'une Authentification forte, l'opération sera considérée comme ayant été validée par le Client, sauf preuve contraire apportée par ce dernier* » (pièce n° 2). Ces CG ont été adressées au CLIENT par courriel le 22 octobre 2023.

La charge de la preuve repose donc, ici, sur le demandeur qui échoue à rapporter la preuve de l'absence de sa négligence, puisqu'il dévoile les faits qui lui sont favorables et reste

silencieux sur les autres circonstances des opérations contestées, et notamment sur celles relatives à la négligence dont il a fait preuve dans la protection de ses données confidentielles.

En l'espèce, ces négligences comprennent notamment :

- la communication de son nouveau mot de passe à son interlocuteur lors de la réinitialisation de celui-ci, communication survenant le cas échéant par l'usage par le CLIENT d'un mot de passe fourni par le fraudeur, alors que la banque Qonto ne fournit jamais de mot de passe qui est une donnée éminemment confidentielle ;
- la validation par le CLIENT de différentes actions sensibles réalisées depuis un appareil autre que le sien : (i) validation de la connexion d'un appareil inconnu ; (ii) validation d'une demande de visualisation de ses coordonnées bancaires confidentielles dont il n'était pas à l'initiative ; et enfin (iii) validation de 6 opérations de paiement successives dont il n'était pas à l'initiative, en pensant, dit-il, annuler lesdites transactions.

Or, sur ce dernier point, la doctrine retient qu'« *est nécessairement fautif celui qui donne son accord à une opération dont il n'est pas à l'origine* ».

Le CLIENT connaît parfaitement le système de paiement en ligne de Qonto puisqu'il a, par le passé, authentifié de nombreuses opérations avec la même notification. Désormais, il allègue qu'il aurait cru, pour la première fois, que ce procédé servait à annuler des transactions qui n'apparaissaient même pas sur son relevé de compte.

En outre le CLIENT a régulièrement été alerté par la BANQUE sur ce type de fraude et sur ce qu'il doit faire et ne pas faire dans un tel cas (pièce n°3).

Et sur les notifications d'opérations pour affichage du numéro de carte, il est clairement indiqué que « *Qonto ne vous demandera jamais et n'enverra jamais d'e-mail pour vous demander d'afficher votre numéro de carte.* »

Contrairement aux dires du CLIENT en demande, l'arrêt de cassation du 23 octobre 2024 confirmant l'arrêt de la cour d'appel de Versailles n'a pas posé le principe d'une « *absence de négligence grave du client dès que l'escroquerie rentre dans le cas d'une situation de spoofing* », et la caractérisation de la négligence relève de l'appréciation in concreto des juges du fond sur laquelle la Cour de cassation n'exerce qu'un contrôle dit « léger », comme précisé par le président Vigneau, président de la chambre commerciale de la Cour de cassation, dans la « *Revue de droit bancaire et financier* » (n°1 du 1<sup>er</sup> janvier 2025).

Sur la caractérisation d'une escroquerie par « spoofing », le demandeur ne rapporte pas la preuve d'avoir identifié le numéro entrant comme étant celui de QONTO, ce numéro n'étant pas mémorisé dans ses contacts.

## LA MOTIVATION

Il ressort des pièces versées au débat le déroulé suivant des opérations durant l'après-midi du 10 janvier 2024 :

- 15h35 Le CLIENT est appelé par le numéro 01 76 41 03 08, par un certain Monsieur BRUN se présentant comme un collaborateur de la BANQUE.  
L'appel téléphonique va durer jusqu'à 16h24, soit 49 minutes.
- 15h39 Un processus de changement de mot de passe est initié depuis un appareil inconnu de Qonto, « inconnu » en ce sens qu'il n'est pas enrôlé sur le compte du CLIENT (réf. « dcd17573-xxxx »)  
Aux dires du CLIENT, il modifie (« réinitialise ») alors son mot de passe en utilisant le mot de passe qui lui est dicté par son interlocuteur au téléphone, à savoir « BLOCAGEFRAUDE1001 ».

- 15h43 La modification du mot de passe est validée par l'appareil de confiance enregistré par Qonto depuis fin 2022 (réf. « 246dc1a0-xxx »)
- 15h44 L'appareil inconnu (réf. dcd17573-xxxx) se présente sur l'espace personnel du CLIENT chez Qonto, en utilisant le mot de passe ainsi réinitialisé.
- 15h45 Le CLIENT autorise l'appareil inconnu à se connecter à son espace client.
- 15h50 L'affichage des informations confidentielles de sa carte bancaire numéro \*\*\*\*[REDACTED] (numéro de 16 chiffres, cryptogramme à 3 chiffres et date d'expiration) est autorisé ; et ce, aux dires de la BANQUE, via une authentification forte et par le CLIENT.
- 15h52 Une transaction de paiement par cette carte bancaire numéro \*\*\*\*[REDACTED] pour 1 759,33 euros (1.992,55 USD) auprès de WIREX est autorisée.
- 15h59 La création d'une carte bancaire virtuelle est validée, numéro \*\*\*\*2990.
- 16h00 L'affichage des informations confidentielles de cette carte bancaire virtuelle numéro \*\*\*\*[REDACTED] (numéro, cryptogramme, date d'expiration) est autorisé.
- 16h01 Une transaction de paiement par cette carte virtuelle numéro \*\*\*\*[REDACTED] de 1.835,82 euros auprès de WIREX est validée.
- 16h03 Une transaction de 9.000 euros auprès de MOONPAY par cette même carte virtuelle numéro \*\*\*\*[REDACTED] est validée.
- 16h14 La création d'une seconde carte bancaire virtuelle numéro \*\*\*\*9767 est validée.
- 16h14 Une demande d'affichage des informations confidentielles de cette seconde carte bancaire virtuelle numéro \*\*\*[REDACTED] (numéro, cryptogramme, date d'expiration) est validée
- 16h16 Une transaction de 1.552,35 euros (1.758,14 USD) auprès de WIREX par cette seconde carte bancaire virtuelle numéro \*\*\*\*[REDACTED] est validée.
- 16h24 L'appel téléphonique prend fin

Enfin, le tribunal note que, le 19 janvier 2024, ont été créditées sur le compte du client au titre des paiements litigieux les sommes 30,76, 4,75 et 18,60 euros en provenance de WIREX.

En l'espèce, le CLIENT nie avoir autorisé les opérations litigieuses en question, alors que le BANQUE prétend rapporter la preuve que ces opérations ont été validées/autorisées par processus avec authentification forte sur l'appareil de confiance enregistré (ou « enrôlé »), à savoir le téléphone de sa gérante, dans le cadre d'une négligence grave.

### **1/ Sur l'opposabilité des « conditions générales » du contrat cadre de services de paiement**

Le défendeur fait valoir les stipulations de l'article 3.3 du « contrat-cadre de services de paiement » qui précisent que :

*« [...] De plus, si le paiement a été initié à la suite d'une Authentification forte, l'opération sera considérée comme ayant été validée par le Client, sauf preuve contraire apportée par ce dernier. ».*

Cependant le CLIENT lui oppose que ce contrat-cadre n'est pas signé et n'a pas été accepté par lui.

Par note en délibéré autorisée par le juge, la BANQUE verse au débat un courriel adressé au CLIENT le 22 octobre 2023, reçu par le CLIENT, par lequel la BANQUE lui adresse les

conditions générales de la convention de compte en question dans sa version applicable au moment des faits (Contrat-cadre de Services de paiement V14 en date du 19/10/2023).

Le CLIENT lui oppose qu'un tel envoi « pour information » ne vaut pas acceptation.

Le tribunal observe que le courriel produit par la BANQUE ne fait aucune référence à une acceptation de ces nouvelles stipulations contractuelles, même à titre tacite en l'absence de réaction du client sous un certain délai.

Et il n'est pas rapporté la preuve d'une autre communication au CLIENT dans ce sens, ni d'une autre sollicitation de ce dernier, ni de conditions générales acceptées à la date d'ouverture du compte bancaire par lesquelles le CLIENT aurait consenti à des modifications à venir des conditions générales communiquée selon ce mode.

Aussi le tribunal retient que ces stipulations ne sont pas non opposables au CLIENT et qu'il sera fait application au présent litige des dispositions applicables du code civil et du code monétaire et financier.

## **2/ Sur le régime de responsabilité applicable aux opérations querellées**

Le régime de la responsabilité du prestataire de services de paiement (ci-après PSP) mise en cause dans le cadre d'une opération de paiement non autorisée ou mal exécutée réalisée au moyen de certains « instruments de paiement » est régi par les articles L. 133-18 et suivants du code monétaire et financier (ci-après CMF), ayant transposé la directive 2015/2366/UE du 25 novembre 2015 (dite directive révisée sur les services de paiement ou DSP2) qui a abrogé la directive précédente 2007/64/CE et qui est entrée pleinement en vigueur le 23 janvier 2018. En application de cette directive, dès lors que la responsabilité d'un PSP est recherchée en raison d'une telle opération de paiement, seul est applicable le régime de responsabilité défini aux articles L. 133-18 à L. 133-24 du CMF, à l'exclusion de tout régime alternatif de responsabilité résultant du droit national.

Les articles L. 133-18 et 133-19 du CMF disposent que

### **Section 6 - Contestation et responsabilité en cas d'opération de paiement non autorisée** **Sous-section 1 - Régime de la responsabilité**

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 au payeur le montant de l'opération non autorisée immédiatement après avoir pris connaissance de l'opération ou après en avoir été informé, et en tout état de cause au plus tard à la fin du premier jour ouvrable suivant, sauf s'il a de bonnes raisons de soupçonner une fraude de l'utilisateur du service de paiement et s'il communique ces raisons par écrit à la Banque de France. Le cas échéant, le prestataire de services de paiement du payeur rétablit le compte débité dans l'état où il se serait trouvé si l'opération de paiement non autorisée n'avait pas eu lieu.*

*[...]*

*En cas de manquement du prestataire de services de paiement aux obligations prévues aux deux premiers alinéas du présent article, les pénalités suivantes s'appliquent :*

*1° Les sommes dues produisent intérêt au taux légal majoré de cinq points ;*

*2° Au-delà de sept jours de retard, les sommes dues produisent intérêt au taux légal majoré de dix points ;*

*3° Au-delà de trente jours de retard, les sommes dues produisent intérêt au taux légal majoré de quinze points.*

*[...] »*

Sous-section 2 - Cas particulier des instruments de paiement dotés de données de sécurité personnalisées

Article L. 133-19

« I. – En cas d'opération de paiement non autorisée consécutive à la perte ou au vol de l'instrument de paiement, le payeur supporte, avant l'information prévue à l'article L. 133-17, les pertes liées à l'utilisation de cet instrument, dans la limite d'un plafond de 50 €.

Toutefois, la responsabilité du payeur n'est pas engagée en cas :

- d'opération de paiement non autorisée effectuée sans utilisation des données de sécurité personnalisées ;
- de perte ou de vol d'un instrument de paiement ne pouvant être détecté par le payeur avant le paiement ;
- de perte due à des actes ou à une carence d'un salarié, d'un agent ou d'une succursale d'un prestataire de services de paiement ou d'une entité vers laquelle ses activités ont été externalisées.

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.

[...]

IV. – Le payeur supporte toutes les pertes occasionnées par des opérations de paiement non autorisées si ces pertes résultent d'un agissement frauduleux de sa part ou s'il n'a pas satisfait intentionnellement ou par négligence grave aux obligations mentionnées aux articles L. 133-16 et L. 133-17.

V. – Sauf agissement frauduleux de sa part, le payeur ne supporte aucune conséquence financière si l'opération de paiement non autorisée a été effectuée sans que le prestataire de services de paiement du payeur n'exige une authentification forte du payeur prévue à l'article L. 133-44.

[...] »

Section 8 - Modalités pratiques et délais en cas d'opérations de paiement non autorisées ou mal exécutées

Article L. 133-23

« 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.

Le prestataire de services de paiement, y compris, le cas échéant, le prestataire de services de paiement fournissant un service d'initiation de paiement, fournit des éléments afin de prouver la fraude ou la négligence grave commise par l'utilisateur de services de paiement. »

Par ailleurs, le paragraphe I de l'article L.133-44 énonce que :

« I. – Le prestataire de services de paiement applique l'authentification forte du client définie au f de l'article L. 133-4 lorsque le payeur :

(...)

2° Initie une opération de paiement électronique ;

*3° Exécute une opération par le biais d'un moyen de communication à distance, susceptible de comporter un risque de fraude en matière de paiement ou de toute autre utilisation frauduleuse. »*

En l'espèce, s'agissant d'une contestation d'opérations de paiements avec utilisation d'un instrument de paiement doté de données de sécurité personnalisées, à savoir en l'espèce une carte bancaire de paiement, le tribunal retient qu'il convient de faire application des cas de responsabilité tels que précisés par l'article L. 133-19 et non seulement du régime général énoncé à l'article L. 133-18.

Aussi le tribunal fera application des régimes de responsabilité tels que prévus à cet article L. 133-19 pour trancher le présent litige.

### **3/ Sur les opérations litigieuses et leur autorisation par authentification renforcée**

Dans le cas d'espèce, il ressort de la pièce n°1 produite par la BANQUE que le CLIENT :

- a un identifiant client : [REDACTED] (= User ID) ;
- a enrôlé en décembre 2022 un appareil de confiance modèle iPhone11 identifié chez la BANQUE par le numéro : [REDACTED] (= Device ID).

Or le tribunal constate qu'ensuite, dans cette pièce n°1, aucun des « logs » relatifs aux opérations litigieuses (changements de mots de passe ; créations de cartes bancaires de paiement virtuelles ; affichages des informations desdites bancaires ; validations des opérations de paiement par carte) ne renvoie à cet identifiant de l'appareil de confiance ; le défendeur citant même dans cette pièce n°1 un autre « Device ID » en page 4 (« Appareil enrôlé du client [REDACTED] »).

Ainsi, au vu des pièces versées aux débats, et notamment de cette pièce n°1 précisant la chronologie des opérations et comprenant les copies d'écran des « logs techniques » par lesquels la BANQUE affirme rapporter la preuve de l'autorisation par un procédé avec authentification forte des opérations litigieuses et de celles qui les auraient précédés, le tribunal constate qu'il lui est impossible de se prononcer sur la pertinence des informations, par ailleurs peu lisibles, qui lui sont présentées et sur leur portée probatoire, en ce compris le fait que la BANQUE affirme, sans le démontrer, que la présence d'un numéro de « event header SCA » dans les « logs techniques » produits démontrerait la validation des opérations concernées par un processus d'authentification forte.

Le tribunal en déduit que la BANQUE échoue à rapporter la preuve d'avoir requis une autorisation des opérations de paiement litigieuses par un procédé avec authentification forte, à partir de l'appareil de confiance enrôlé par le CLIENT ou par un appareil autorisé par lui, en violation des dispositions du paragraphe I de l'article L. 133-44 du CMF.

Par ailleurs, la BANQUE ne met pas au débat un agissement frauduleux de la part du CLIENT, circonstance qui lui aurait, le cas échéant, permis de se soustraire aux dispositions du paragraphe V de l'article L. 133-19 du CMF.

En conséquence, et sans qu'il soit besoin pour le tribunal d'analyser ni de déterminer les circonstances exactes de réalisation par le fraudeur, sans défaillance technique, des opérations contestées et de celles qui ont précédé, ni de rechercher une éventuelle négligence grave du CLIENT dans ce cadre, le tribunal fera application des dispositions du paragraphe V de l'article L. 133-19 du CMF et, faisant droit aux prétentions de ce dernier, il condamnera la BANQUE à lui payer la somme de 14 093,39 euros (= 14.147,50 - 30,76 - 4,75 - 18,60).

Comme demandé, il sera fait application des pénalités prévues dans ce cas par l'article L. 133-18 à compter du 10 janvier 2024, à savoir :

- des intérêts au taux légal majoré de cinq points jusqu'au 17 janvier 2024 ;
- des intérêts au taux légal majoré de dix points jusqu'au 9 février 2024 ;
- puis des intérêts au taux légal majoré de quinze points après cette date.

La capitalisation des intérêts étant demandée, le tribunal l'ordonnera dans les conditions de l'article 1343-2 du code civil, de sorte que les intérêts porteront eux-mêmes intérêts dès lors qu'ils seront dus pour une année entière.

#### **4/ Sur la demande de dommages et intérêts pour résistance abusive**

Face au refus abusif de la BANQUE de lui rembourser le montant des opérations litigieuses débitées, le CLIENT demande que celle-ci soit condamnée à lui payer la somme de 3.000 euros à titre de dommages et intérêts pour résistance abusive.

Il appartient donc au CLIENT de prouver la faute de la BANQUE, de préciser la nature du préjudice subi, d'en justifier le quantum et enfin de démontrer le lien causal entre la faute et le préjudice

Ni les circonstances du litige, ni les éléments de la procédure ne permettent de caractériser à l'encontre de la BANQUE une faute de nature à faire dégénérer en abus le droit de se défendre en justice.

En outre, dans l'hypothèse où le refus de remboursement de la part de la BANQUE pourrait être analysé comme fautif ou abusif, le CLIENT ne justifie pas d'un préjudice distinct de celui dont il obtiendra réparation par les pénalités (intérêts de retard) mises à la charge de la BANQUE et par la condamnation qui sera prononcée en application des dispositions de l'article 700 du code de procédure civile.

Aussi il ne sera pas fait droit à la demande de dommages intérêts formée à ce titre.

#### **5/ Sur les dépens, les frais irrépétibles et l'exécution provisoire**

Les dépens seront mis à la charge de la BANQUE, partie perdante au sens de l'article 696 du code de procédure civile.

De plus, le CLIENT a dû, pour faire reconnaître ses droits, exposer des frais non compris dans les dépens et le tribunal condamnera la BANQUE à lui payer la somme de 2.500 euros, à titre d'indemnité sur le fondement de l'article 700 du code de procédure civile, déboutant pour le surplus.

L'exécution provisoire étant de droit et aucune partie ne demandant à l'écartier, il n'y aura pas lieu de statuer.

#### **PAR CES MOTIFS**

Le tribunal statuant publiquement par jugement contradictoire en premier ressort :

- condamne la société OLINDA à payer à la société [REDACTED] les sommes de :
  - o 14 093,39 euros au titre des opérations contestées, avec pénalités telles que prévues à l'article L. 133-18 à compter du 10 janvier 2024, à savoir :
    - des intérêts au taux légal majoré de cinq points jusqu'au 17 janvier 2024,
    - des intérêts au taux légal majoré de dix points jusqu'au 9 février 2024,
    - puis des intérêts au taux légal majoré de quinze points après cette date,

- 2.500 euros à titre d'indemnité en application de l'article 700 du code de procédure civile,
- ordonne la capitalisation de ces intérêts en application de l'article 1343-2 du code civil,
- déboute la société [REDACTED] de sa demande de dommages et intérêts pour résistance abusive.
- condamne la société OLINDA aux dépens, dont ceux à recouvrer par le greffe, liquidés à la somme de 70,86 € dont 11,60 € de TVA.

En application des dispositions de l'article 871 du code de procédure civile, l'affaire a été débattue le 27 novembre 2025, en audience publique, devant M. Emmanuel Ramé, juge chargé d'instruire l'affaire, les représentants des parties ne s'y étant pas opposés.

Ce juge a rendu compte des plaidoiries dans le délibéré du tribunal, composé de : M. Emmanuel Ramé, M. Vincent Tricon et M. Laurent Pfeiffer.

Délibéré le 18 décembre 2025 par les mêmes juges.

Dit que le présent jugement est prononcé par sa mise à disposition au greffe de ce tribunal, les parties en ayant été préalablement avisées lors des débats dans les conditions prévues au deuxième alinéa de l'article 450 du code de procédure civile.

La minute du jugement est signée par M. Emmanuel Ramé, président du délibéré et par Mme Elisabeth Gonçalves, greffier.

Le greffier

Le président