**Texte pseudonymisé**

**Avertissement: Ce document pseudonymisé a une valeur purement informative. Le document original seul fait foi.**

Répertoire n° 179/26
Dossier n° L-CIV-527/25

**Audience publique du 15 janvier 2026**

Le Tribunal de Paix de et à Luxembourg, arrondissement judiciaire de Luxembourg, siégeant en matière civile, a rendu le jugement qui suit :

dans la cause entre

**PERSONNE1.),** demeurant à D-ADRESSE1.),

**partie demanderesse,**

comparant par Maître Ugo MONMARTY, avocat, en remplacement de Maître Cathy ARENDT, avocat, les deux demeurant à Luxembourg,

et

**la société anonyme SOCIETE1.),** établie et ayant son siège social à L-ADRESSE2.), inscrite au Registre de Commerce et des Sociétés de Luxembourg sous le numéro NUMERO1.), représentée par son conseil d'administration actuellement en fonctions,

**partie défenderesse,**

comparant par la société anonyme SCHILTZ & SCHILTZ SA, établie et ayant son siège social à L-1610 Luxembourg, 24-26, Avenue de la Gare, inscrite au Barreau de Luxembourg, immatriculée au Registre de Commerce et des Sociétés de PERSONNE3.)embourg sous le numéro B220251, représentée pour les besoins de la présente procédure par Maître Lison MERGAUX, avocat, en remplacement de Maître Franz SCHILTZ, avocat, les deux demeurant à PERSONNE3.)embourg.

---

## Faits

Par exploit du 26 septembre 2025 de l'huissier de justice Geoffrey GALLÉ, PERSONNE1.) a fait donner citation à la société anonyme SOCIETE1.) à comparaître devant le Tribunal de Paix de et à PERSONNE3.)embourg à

l'audience publique du jeudi, 16 octobre 2025 à 15.00 heures, salle JP.1.19, pour y entendre statuer conformément à la citation prémentionnée et annexée à la minute du présent jugement.

Cette affaire fut enrôlée sous le numéro L-CIV-527/25.

A l'audience publique du 16 octobre 2025, l'affaire fut fixée pour plaidoiries à l'audience publique du jeudi, 11 décembre 2025 à 15.00 heures, salle JP.0.02.

A l'audience publique du 11 décembre 2025, le mandataire de PERSONNE1.), Maître Ugo MONMARTY, avocat, en remplacement de Maître Cathy ARENDT, avocat, et la mandataire de la société anonyme SOCIETE1.), Maître Lison MERGAUX, avocat, en remplacement de Maître Franz SCHILTZ, avocat, furent entendus en leurs moyens et conclusions.

Sur ce, le Tribunal prit l'affaire en délibéré et fixa le prononcé à l'audience publique du 8 janvier 2026.

Le 8 janvier 2026 le prononcé fut remis à l'audience publique du 15 janvier 2026 lors de laquelle fut rendu le

**le jugement qui suit :**

Par exploit du 26 septembre 2025 de l'huissier de justice Geoffrey GALLÉ, PERSONNE1.) a fait donner citation à la société anonyme SOCIETE1.) (ci-après la « SOCIETE1.) ») à comparaître devant le Tribunal de Paix de et à Luxembourg pour la voir condamner à lui payer le montant de 9.999,- euros avec les intérêts légaux à compter de la demande en justice et jusqu'à solde et le montant d'un euro symbolique à titre de préjudice moral. Il réclame en outre une indemnité de procédure de 1.000,- euros sur base de l'article 240 du nouveau code de procédure civile et la condamnation de la SOCIETE1.) aux frais et dépens de l'instance ainsi que l'exécution provisoire de la condamnation pécuniaire à intervenir.

Aux termes de la citation, PERSONNE1.) soutient avoir reçu, le 23 avril 2025, vers 10 heures du matin, une notification sur son téléphone portable, mentionnant le prélèvement d'un montant de 4.500,- euros dont il ne connaissait absolument pas l'objet.

Il se serait rapidement et directement rendu sur la page du site internet de la SOCIETE1.), via un signet déjà utilisé plusieurs fois auparavant, afin d'accéder à son espace personnel. La saisie du mot de passe et du token SOCIETE2.) auraient échoué à plusieurs reprises, ce qui ne lui aurait pas paru inhabituel. Il aurait insisté à deux ou trois reprises et se serait rendu compte de deux nouvelles notifications sur son téléphone concernant l'annulation de deux virements différents.

Une employée de la SOCIETE1.), Madame PERSONNE2.), aurait appelé PERSONNE1.) et lui aurait demandé si le virement du montant de 4.500,- euros

provenait de lui, ce qu'il aurait contesté. La SOCIETE1.) l'aurait informé qu'elle bloquait ledit virement.

PERSONNE1.) aurait informé son interlocutrice de ses difficultés d'accéder au site internet de la SOCIETE1.). Cette-dernière lui aurait signalé un autre virement de 9.999,- euros. PERSONNE1.) aurait confirmé que ce virement ne provenait pas de lui. Son interlocutrice lui aurait dit qu'elle procèderait au blocage du virement. PERSONNE1.) aurait été rappelé par son établissement bancaire pour lui signaler que tout avait été bloqué. Il lui était également recommandé d'annuler ses cartes de crédit, le certificat SOCIETE2.) et de bloquer son compte, ce que PERSONNE1.) aurait fait.

Le 25 avril 2025, PERSONNE1.) aurait reçu les données d'accès de son nouveau certificat SOCIETE2.). Le 28 avril 2025, PERSONNE1.) serait parvenu à se connecter à son nouveau compte en ligne et il aurait constaté que le montant de 9.999,- euros avait tout de même été débité.

Le service des fraudes de la SOCIETE1.) l'aurait informé que le remboursement pourrait prendre jusqu'à cinq semaines, avec une possibilité que l'argent ne lui soit pas restitué.

PERSONNE1.) tentait de contacter l'établissement bancaire vers lequel le transfert de 9.999,- euros avait été fait, la banque SOCIETE3.), en vain. En parallèle, il n'arrivait plus à joindre la SOCIETE1.) par téléphone, en raison d'une longue file d'attente téléphonique.

Très compréhensif, mais néanmoins inquiet, PERSONNE1.) aurait écrit, le 30 avril 2025, un message à la SOCIETE1.) via la plateforme sécurisée afin de signaler que le montant de 9.999,- euros n'avait toujours pas été recrédité sur son compte.

Le 2 mai 2025, PERSONNE1.) contactait par téléphone l'établissement bancaire SOCIETE3.) (banque ayant reçu le montant), qui lui indiquait que, n'étant pas client, ils ne pouvaient rien faire pour lui et qu'il devait alors s'adresser à son propre établissement bancaire.

Il était alors rappelé par la SOCIETE1.) qui lui indiquait que cette dernière ne pourrait diligenter une enquête interne qu'après réception de la copie d'un dépôt de plainte.

Le jour même à 15h15, PERSONNE1.) déposait plainte au commissariat et relatait les faits tels que décrits ci-dessus. Il y indiquait notamment que ce n'est que plus tard qu'il s'était rendu compte que le site internet sur lequel il s'était rendu avait une adresse URL se terminant par « .cc » et non par « .lu ».

Le signet aurait été enregistré par PERSONNE1.) il y a plusieurs années et le site internet vers lequel renvoyait ce signet était la reproduction, à l'identique, du site officiel de la SOCIETE1.). Il ne saurait donc être valablement soutenu que l'utilisation d'un moteur de recherches de type ALIAS1.) pour se connecter à son espace personnel bancaire serait une négligence grave de sa part, surtout

lorsque le site internet falsifié était véritablement ouvragé pour tromper les utilisateurs les plus alertes.

Le 12 juin 2025, la SOCIETE1.) n'aurait pas manqué de souligner l'erreur de PERSONNE1.) ainsi que son refus de procéder au remboursement du montant de 9.999,- euros sur le fondement de l'article 88, alinéa 2, de la loi du 10 novembre 2009 relative aux services de paiement, ce pour *« négligence »* du demandeur.

En outre, et *a contrario* des explications de PERSONNE1.) dans son dépôt de plainte, la SOCIETE1.) indiquait que PERSONNE1.) « *avait probablement répondu à un e-mail ou à un SMS frauduleux dans les jours ou les heures qui ont précédé l'incident* ».

Le 31 juillet 2025, PERSONNE1.) adressait à la SOCIETE1.), par l'intermédiaire de Maître ARENDT, un courrier rappelant le déroulement des faits, notamment l'utilisation d'un signet (ou Bookmark) et sollicitant le remboursement de la somme litigieuse, notamment en raison du fait que les pays de destination des virements qu'il faisait, et qu'il avait dû indiquer à la SOCIETE1.), étaient uniquement le Luxembourg, l'Allemagne et l'Autriche. A cet égard, il ressort de la copie du dépôt de plainte que les virements ont été faits à destination de la France, ce qui ne correspond pas au profil de PERSONNE1.), malgré les allégations de la SOCIETE1.) dans le courrier du 12 juin précité. Le même jour, PERSONNE1.), logiquement agacé et angoissé de cette situation, sollicitait de la SOCIETE1.) la désactivation de l'instantanéité des transferts. La SOCIETE1.) aurait produit une réponse d'attente le 7 août 2025. Le 18 août 2025, la SOCIETE1.) répondait à Maître ARENDT, sur le fait que PERSONNE1.) était victime d'un faux site, que « *A moins d'avoir tapé à la main l'adresse du faux site lors de la création du bookmark, il* [PERSONNE1.)] *est passé par un moteur de recherche qui lui a indiqué le site falsifié dans les premiers résultats de recherche* », ce qui changeait pour le moins radicalement, de leur supposition précédente de réponse à un SMS ou à un email frauduleux, du 12 juin 2025. Pour le reste, la SOCIETE1.) maintenait sa position de refus quant au remboursement la somme litigieuse, toujours au motif que le demandeur avait commis une *« négligence »*. Raison pour laquelle PERSONNE1.) a fait citer la SOCIETE1.).

La SOCIETE1.) considérant, dans ses deux courriers précités, et sur le fondement de l'article 88, alinéa 2, de la loi du 10 novembre 2009 relative aux services de paiement, que PERSONNE1.) aurait fait preuve de *« négligence »*.

A cet égard, la négligence serait définie comme « tout comportement défectueux qui, étant préjudiciable à autrui, trouble la paix sociale » (G. Ravarani, La responsabilité civile des personnes privées et publiques, 2e éd., n o 70).

Or, dans les deux courriers litigieux, la SOCIETE1.) semblerait avoir légèrement omis de prendre en compte, dans le cadre de son analyse, l'entièreté du cadre législatif.

En effet, l'article 88, alinéa 2, de la loi du 10 novembre 2009 sur les services de paiement, énonçant notamment 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 du fait que le payeur n'a pas satisfait, intentionnellement ou à la suite d'une négligence grave, à une ou plusieurs des obligations qui lui incombent en vertu de l'article 83* ». Il y aurait donc lieu de constater que, loin d'une simple négligence, le texte sur lequel la SOCIETE1.) se fonde traite de *« négligence grave »*.

La loi du 10 novembre 2009 précitée étant la transposition de la Directive (UE) 2007/64/CE du 13 novembre 2007 (la « Directive Paiement »), dont l'article 61 est la réplique exacte de l'article 88 de ladite loi. Or, le considérant 32 de cette Directive Paiement traite également bien de *« négligence grave »*, tandis que le considérant 33 énonce, quant à lui, que :

« *Afin d'évaluer l'éventualité d'une négligence de la part de l'utilisateur de services de paiement, il convient de tenir compte de toutes les circonstances. Les preuves et le degré de négligence supposée devraient être évalués conformément au droit national. Les clauses et conditions contractuelles concernant la fourniture et l'utilisation d'un instrument de paiement qui auraient pour effet d'alourdir la charge de la preuve incombant au consommateur ou d'alléger la charge de la preuve imposée à l'émetteur devraient être considérées comme nulles et non avenues.* »

La Directive (UE) 2015/2366 du 25 novembre 2015 (la « Directive Paiement 2 ») venant abroger la Directive Paiement et, sans aucune modification au contenu du texte qui nous intéresse, hors une simple renumérotation, précise, en son considérant 72 sur cette question que :

« *Afin d'évaluer l'éventualité d'une négligence ou d'une négligence grave de la part de l'utilisateur de services de paiement, il convient de tenir compte de toutes les circonstances. Les preuves et le degré de négligence alléguée devraient en général être évalués conformément au droit national. Toutefois, si la négligence implique un manquement au devoir de diligence, la négligence grave devrait impliquer plus que de la simple négligence et comporter un défaut de vigilance caractérisé, comme le serait le fait de conserver les données utilisées pour autoriser une opération de paiement à côté de l'instrument de paiement, sous une forme aisément accessible et reconnaissable par des tiers (…) En outre, dans des situations spécifiques et en particulier lorsque l'instrument de paiement n 'est pas présent au point de vente, par exemple dans le cas de paiements en ligne, il convient que le prestataire de services de paiement soit tenu d'apporter la preuve de la négligence alléguée, le payeur n'ayant, dans ce cas, que des moyens limités de le faire* ».

A cet égard, outre le fait que PERSONNE1.) n'a jamais répondu à un quelconque email ou SMS frauduleux, comme supposé à tort pour refuser l'indemnisation dans le courrier de la SOCIETE1.) en date du 12 juin 2025, il ne serait pas non plus démontré :

-d'une part, que la précaution, selon laquelle les moteurs de recherches tels que ALIAS1.) ne devaient pas être utilisés, était préalablement renseignée, au sein des conditions générales de la SOCIETE1.). Au contraire, lesdites conditions

générales applicables à compter du 1er janvier 2025 n'en font manifestement pas état ;

-d'autre part, que l'encart informatif du site internet de la SOCIETE1.) sur cette précaution ait été porté à la connaissance des clients de l'établissement avant que cette affaire ne défraie la chronique.

En tout état de cause, et même dans l'éventualité où PERSONNE1.) aurait utilisé un moteur de recherches de type ALIAS1.) et se soit rendu compte, peu de temps après, que ledit site internet se terminait par « .cc » et non par «.lu» ou « .com », cela ne pourrait être constitutif que d'une simple négligence, et non de la négligence grave requise par le droit luxembourgeois, en application des directives européennes.

La négligence grave de PERSONNE1.) laisserait d'être démontrée.
Il y aurait lieu de condamner la SOCIETE1.) à rembourser à celui-ci le montant de 9.999,- euros frauduleusement débitée de son compte bancaire.

La chronologie des faits ne pourrait que laisser dubitatif quant à une négligence dans le fonctionnement opérationnel de cet établissement bancaire, *i.e.* ne pas avoir alerté plus tôt PERSONNE1.) du virement de 9.999,- euros alors qu'il s'agissait, sinon d'un virement suspect, d'un virement à tout le moins atypique.

L'article 86 (2) de la loi du 10 novembre 2009 relative aux services de paiement dispose que : « *Lorsqu'un utilisateur de services de paiement nie avoir autorisé une opération de paiement qui a été exécutée, l'utilisation d'un instrument de paiement, telle qu'enregistrée par le prestataire de services de paiement, ne suffit pas nécessairement en tant que telle à prouver que I 'opération de paiement a été autorisée par le payeur ou que celui-ci a agi frauduleusement ou n'a pas satisfait, intentionnellement ou à la suite d'une négligence grave, à une ou plusieurs des obligations qui lui incombent en vertu de l'article 83*. »

La jurisprudence française a pu considérer qu'il ne pouvait pas se déduire de l'utilisation effective de l'instrument de paiement ou des données personnelles qui lui sont liées, l'existence d'une négligence grave (Cass. Fr., Com., 21 novembre 2018, 11017-18.888).

Il ne ferait nul doute que la SOCIETE1.) se réfugie derrière le système d'authentification forte par l'utilisation d'un certificat SOCIETE2.). Or, et sauf à renverser la charge de la preuve, il appartient à la SOCIETE1.) de prouver tant l'absence de défaillance de son système d'authentification des opérations en ligne, que les négligences, qui se doivent d'être *« graves »*, qu'elle impute à PERSONNE1.).

Les termes des correspondances de la SOCIETE1.) ne manqueraient pas de laisser dubitatif, notamment quant à l'affirmation péremptoire selon laquelle Madame PERSONNE2.) aurait alerté PERSONNE1.) de ce que le premier virement avait déjà été débité et qu'elle ne pouvait plus l'arrêter, ce qui est catégoriquement nié par le demandeur à la présente instance, de façon circonstanciée, et qui n'est à aucun moment démontré par la SOCIETE1.).

L'affirmation selon laquelle *« l'application SOCIETE2.) lui* [PERSONNE1.)] *a indiqué la transaction qu'il s'agissait de signer (ouverture d'une session SOCIETE1.)) transfert...) »* et *« en cas d'un transfert »*, ce dont la SOCIETE1.) n'est manifestement pas certaine, le montant et le bénéficiaire étaient également indiqués, n'est nullement démontrée.

Il serait étonnant que PERSONNE1.) ait immédiatement réagi à la notification pour un virement d'un montant de « seulement » 4.500,- euros, de même que Madame PERSONNE2.) ait téléphoné à Monsieur PERSONNE1.) pour ce même virement, sans qu'il y ait eu un appel antérieur de l'un à l'autre, et qu'un virement plus important de 9.999,- euros ait pu être immédiatement débité sans qu'il n'y ait eu aucune alerte de la part de la SOCIETE1.), et alors que le transfert d'un tel montant vers un compte bancaire en France était clairement atypique par rapport au profil du demandeur.

Il ne serait à aucun moment contesté que Madame PERSONNE2.) ait informé PERSONNE1.) de l'existence d'un virement de 9.999,- euros, ce qui démontrerait, si nécessaire, que cette dernière a également considéré ce virement comme suspect ou, à tout le moins, atypique.

Dès lors, il serait évident que les affirmations de la SOCIETE1.) laissent d'être démontrées et que ses correspondances ne répondent pas au critère de justification mentionné à l'article 90 de la Loi du 10 novembre 2009 précitée.

La SOCIETE1.) y répond aux termes d'une note de plaidoiries ce qui suit.

PERSONNE1.), d'après ses explications, aurait reçu le 23 avril 2025 une notification sur son téléphone, l'informant d'un prélèvement de 4.500,- euros.

PERSONNE1.) se serait ensuite connecté, via l'application SOCIETE2.), à un prétendu site SOCIETE1.). A ce titre, PERSONNE1.) indique que la saisie du mot de passe et du token SOCIETE2.) a échoué à plusieurs reprises, mais que ça ne lui aurait pas paru inhabituel (p. 2 de l'assignation). PERSONNE1.) se serait par la suite rendu compte que le prétendu site SOCIETE1.) sur lequel il s'est connecté avait une adresse URL se terminant par « .cc » et non par « .lu ».

PERSONNE1.) aurait ensuite reçu un appel de Madame Lux de la SOCIETE1.) lui demandant s'il voulait effectuer le virement de 4.500,- euros qui avait été initié sur son compte bancaire. PERSONNE1.) lui ayant alors indiqué qu'il ne voulait pas effectuer un tel virement, Madame Lux aurait pu bloquer le virement à temps. A ce moment, Madame Lux s'est rendu compte et a informé PERSONNE1.) qu'un autre virement de 9.999,- euros avait d'ores et déjà été effectué à partir de son compte bancaire. Le montant avait déjà été débité et qu'il n'était plus possible de le bloquer.

Trois virements auraient été effectués depuis le compte bancaire de PERSONNE1.) le 23 avril 2025, le 1er de 9.999,- euros et les deux autres de 4.500,- euros chacun (qui ont pu être bloqués grâce à la vigilance de la SOCIETE1.)). Ces trois virements étaient en faveur d'un compte bancaire

français appartenant à un dénommé PERSONNE4.). La partie défenderesse se baserait uniquement ici sur sa pièce n° 2 versée par elle, et non sur les captures d'écran de l'historique bancaire versées par PERSONNE1.) lui-même qui ne seraient pas clairs et sur lesquels il serait notamment question d'un prétendu PERSONNE5.), lequel n'apparaît manifestement à aucun endroit sur les relevés de la SOCIETE1.).

La SOCIETE1.) tient à relever que les faits tels que relatés par PERSONNE1.) demeurent à ce stade assez flou, certaines informations essentielles quant au déroulé des faits ayant certainement été omises. Demeurerait à ce stade notamment inconnu :

- la forme de la notification reçue par PERSONNE1.) sur son téléphone, depuis quel/quelle site/application cette notification est intervenue ? ;

- l'adresse URL complète du prétendu site internet SOCIETE1.).

Quoi qu'il en soit, et sur base des seules explications de PERSONNE1.), la partie défenderesse conteste l'ensemble des demandes.

La SOCIETE1.) soutient avant tout et surtout qu'il y aurait lieu de constater que le virement de 9.999,- euros, effectué depuis le compte bancaire de la partie demanderesse le 23 avril 2025 et pour lequel la partie demanderesse demande remboursement, a été autorisé par la partie demanderesse elle-même, de sorte que ce virement n'est pas à considérer comme « opération non autorisée » au sens de loi luxembourgeoise sur les services de paiement du 10 novembre 2009.

En effet, le point (1) de l'article 81 intitulé « *Le consentement et le retrait du consentement* » de la loi luxembourgeoise sur les services de paiement du 10 novembre 2009 dispose :

« *(1) Une opération de paiement n'est réputée autorisée que si le payeur a donné son consentement à l'exécution de l'opération de paiement. Une opération de paiement peut être autorisée par le payeur avant ou, si le payeur et le prestataire de services de paiement en ont convenu ainsi, après son exécution* ».

L'article 80 intitulé « *Contestations* » des conditions générales de la banque stipule encore :

« *Si le client estime qu'une opération de paiement n'aurait pas été autorisée par lui, c'est à lui d'en rapporter la preuve. Jusqu'à preuve du contraire, une opération exécutée est réputée avoir été autorisée par le client* ».

En l'espèce, et contrairement à ce que tenterait de faire croire la partie demanderesse, elle aurait donné son consentement à l'exécution du virement de 9.999,- euros.

En effet, il résulterait de la pièce n°1 de la défenderesse, reprenant l'analyse technique du virement, que le virement a été validé grâce à l'introduction par PERSONNE1.) lui-même de ses identifiants SOCIETE2.).

Ceci serait encore corroboré par le fait que PERSONNE1.) indique lui-même avoir à plusieurs reprises, lorsqu'il tentait de se connecter au prétendu site SOCIETE1.), entré ses données et validé via son token SOCIETE2.). A ce moment-là PERSONNE1.) aurait validé lui-même l'opération en question.

La partie demanderesse aurait ainsi dûment autorisé la transaction, la partie demanderesse ne rapportant pas la moindre preuve contraire.

L'on ne se trouverait donc manifestement pas, et contrairement aux dires adverses, en l'espèce dans un cas qui pourrait induire une obligation de prise en charge par la SOCIETE1.).

S'agissant donc d'une opération dûment autorisée, il n'y a pas lieu de faire droit à la demande d'indemnisation adverse (qui reste contestée tant dans son principe que dans son quantum), un tel droit au remboursement n'étant pas consacré par la loi de 2009.

A titre subsidiaire, et s'il y avait lieu d'appliquer les dispositions de la loi luxembourgeoise sur les services de paiement du 10 novembre 2009, quod non, malgré le fait qu'il s'agisse d'une opération de paiement dûment autorisée, la partie défenderesse prend position comme suit :

La partie demanderesse continue de nier avoir autorisé le virement de 9.999,- euros et demande que la partie défenderesse soit condamnée à lui rembourser ce montant sur base de l'article 26 (2) de la loi luxembourgeoise sur les services de paiement du 10 novembre 2009 (?!) ainsi que sur les articles 1146 et suivants du Code civil, sinon sur base des articles 1382 et 1383 du code civil.

L'article 86 intitulé « *La preuve d'authentification et d'exécution des opérations de paiement* » de la loi luxembourgeoise sur les services de paiement du 10 novembre 2009 dispose :

« *(1) 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 au 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 du service fourni par le Prestataire de services de paiement.*

*Si l'opération de paiement est initiée par l'intermédiaire d'un prestataire de services d'initiation de paiement, c'est à ce dernier qu'incombe la charge de prouver que, pour ce qui le concerne, l'opération en question a été authentifiée et dûment enregistrée et qu'elle n'a pas été affectée par une déficience technique ou autre en relation avec le service de paiement qu'il doit assurer.*

*(2) Lorsqu'un utilisateur de services de paiement nie avoir autorisé une opération de paiement qui a été exécutée, l'utilisation d'un instrument de paiement, telle qu'enregistrée par le prestataire de services de paiement, y compris le prestataire de services d'initiation de paiement, le cas échéant, ne suffit pas nécessairement*

*en tant que telle à prouver que l'opération de paiement a été autorisée par le payeur ou que celui-ci a agi frauduleusement ou n'a pas satisfait, intentionnellement ou à la suite d'une négligence grave, à une ou plusieurs des obligations qui lui incombent en vertu de l'article 83. Le prestataire de services de paiement, y compris le cas échéant, le prestataire de services d'initiation de paiement, fournit des éléments afin de prouver la fraude ou la négligence grave commise par l'utilisateur de services de paiement ».*

L'article 86 de la loi luxembourgeoise sur les services de paiement du 10 novembre 2009 étant similaire à l'article L-133-23 du code monétaire et financier français, il y aurait lieu de se référer à la jurisprudence française en la matière :

« *En premier lieu, 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.* ».

Ainsi, le prestataire de services de paiements doit donc démontrer :

-d'une part, que l'opération de paiement litigieuse a été rendue possible par un manquement de l'utilisateur ;

-d'autre part, qu'il a correctement exécuté cette opération, c'est-à-dire que l'opération a été authentifiée, dûment enregistrée et comptabilisée et qu'elle n'a pas été affectée par une déficience technique ou autre.

La preuve que l'opération a été authentifiée, dûment enregistrée et comptabilisée et qu'elle n'a pas été affectée par une déficience technique ou autre résulte du fait même que la transaction a été dûment autorisée par la partie demanderesse elle-même, laquelle a signé cette transaction grâce à son SOCIETE2.).

La pièce n°1 qui montrerait l'analyse technique du virement et dont résulte l'authenticité de cette opération, sa comptabilisation et son enregistrement corrects.

Renvoi est également fait aux déclarations faites par la partie demanderesse elle-même qui reconnaît avoir à plusieurs reprises, en tentant de se connecter au prétendu site SOCIETE1.), entré ses données et validé via son token SOCIETE2.).

Quant à la preuve d'un manquement dans le chef de la partie demanderesse, suivant l'article 83 intitulé « *Les obligations de l'utilisateur de services de paiement liées aux instruments de paiement et aux données de sécurité*

*personnalisées* » de la loi du 10 novembre 2009 relative aux services de paiement :

« *(1) L'utilisateur de services de paiement habilité à utiliser un instrument de paiement a les obligations suivantes :*

*a) il utilise l'instrument de paiement conformément aux conditions régissant l'émission et l'utilisation de cet instrument de paiement, qui doivent être objectives, non discriminatoires et proportionnées ; et*

*b) lorsqu'il a connaissance de la perte, du vol du détournement ou de toute utilisation non autorisée de son instrument de paiement, il en informe sans tarder son prestataire de services de paiement ou l'entité désignée par celui-ci.*

*(2) Aux fins du paragraphe (1), point a), dès qu'il reçoit un instrument de paiement l'utilisateur de services de paiement prend notamment toute mesure raisonnable pour préserver la sécurité de ses données de sécurité personnalisées.* »

Suivant l'article 87 intitulé « *Responsabilité du client* » des conditions générales de la banque (pièce n°14 de la partie demanderesse) :

*« Le client doit veiller à garder strictement confidentiels tous les Codes Personnels et à ne les inscrire sur aucun document. Il s'engage à n'enregistrer que ses propres données biométriques sur son appareil dans le cadre de l'authentification via l'utilisation de données biométriques. Il s'engage en outre à respecter toutes les recommandations de l'émetteur du Moyen de Connexion, destinées à préserve la sécurité de ses Codes Personnels, de même que les principes en matière de sécurité repris sur SOCIETE1.). Il incombe exclusivement au client (i) de révéler ses Codes Personnels aux AIPS ou aux PISP aux fins de la délivrance des services par ces derniers ainsi que de veiller à ce que, lorsqu'ils utilisent ces Codes Personnels, les AIPS ou PISP respectent les dispositions de la présente section VI et (ii) de choisir son mot de passe et (iii) de protéger ses Codes Personnels contre toute erreur ou imprudence.*

*Le client peut avoir accès aux services SOCIETE1.) par tout moyen adéquat quel que soit son emplacement. Afin de réduire les risques d'accès par des personnes non autorisées aux codes confidentiels d'accès du client celui-ci ne doit se connecter que directement à SOCIETE1.) et non pas indirectement p. ex. à travers des liens. Tout accès indirect par le client au site internet de la Banque se fait à ses propres risques. Internet se présente comme un réseau international ouvert, dont la structure et les spécificités sont connues du client. La Banque a pris les mesures nécessaires afin de garantir un traitement sécurisé des opérations via internet. La Banque n'assume qu'une obligation de moyens dans ce domaine* ».

Contrairement à ce que tenterait de faire croire la partie demanderesse, la SOCIETE1.) aurait bien mis en garde ses clients quant aux risques de se connecter aux services SOCIETE1.) de manière indirecte, tel que l'a fait en

l'espèce la partie demanderesse en s'y connectant via un moteur de recherches internet.

La partie demanderesse n'aurait manifestement pas pris les mesures de sécurité nécessaires qui, suivant la loi et les conditions générales de la banque, s'imposaient à elle afin d'éviter toute fraude, de sorte que la SOCIETE1.) ne saurait être tenue responsable.

Il résulterait en effet des explications données par la partie demanderesse, mais aussi de la plainte pénale (pièce n°8 de la partie demanderesse) que la partie demanderesse a manifestement commis plusieurs imprudences constitutives de négligences graves au sens de la loi du 10 novembre 2009.

D'après la partie demanderesse elle-même :

-elle aurait utilisé le moteur de recherches ALIAS1.), pour tenter de se connecter à SOCIETE1.), elle aurait tenté de s'y rendre de manière indirecte, ce qui est contraire aux recommandations de la SOCIETE1.) ;

-elle aurait entré ses données en tentant de se connecter à ce prétendu site SOCIETE1.), données qu'elle a validées via son token SOCIETE2.) ;

-elle aurai entré ses données à plusieurs reprises bien que la connexion ait échoué ;

-elle n'aurait pas vérifié l'adresse URL du faux site sur lequel elle s'est rendue de manière indirecte.

En tout état de cause, la validation via SOCIETE2.) vaut preuve de l'accord du client et donc ordre de procéder au virement. Il appartiendrait donc à la partie demanderesse de supporter les conséquences en termes de transaction frauduleuse, la partie demanderesse ayant elle-même procédé au virement.

En agissant de la sorte, la partie demanderesse a permis au malfaiteur de recevoir les 9.999,- euros. Elle aurait dû être plus méfiante et ne pas commettre les négligences graves répétées telles qu'énoncées.

Ce ne serait pourtant pas faute pour la banque d'avoir, via les nombreuses campagnes de sensibilisation, attiré l'attention des clients sur les risques de fraude.

Un utilisateur normalement attentif et prudent ne se serait pas, dans une situation comme en l'espèce, rendu via un moteur de recherches sur le (prétendu) site de la SOCIETE1.) sans en vérifier l'adresse URL et n'aurait surtout pas continué d'entrer ses données à plusieurs reprises alors que la connexion a échoué.

La partie demanderesse prétendant encore que le virement de 9.999,- euros, validé par la partie demanderesse elle-même (!) serait un virement suspect, ou en tout cas atypique. Or, il résulterait de la pièce n°10 de la partie défenderesse

qu'au vu de l'historique des virements de la partie demanderesse, un virement de 9.999,- euros ne serait absolument pas inhabituel, bien au contraire.

Il ne saurait pas non plus être retenu d'une quelconque manière qu'un virement vers un compte bancaire français ait un caractère atypique, alors que la France n'est pas un pays identifié par le GAFI comme à risque. Il convient encore de préciser que l'allégation adverse suivant laquelle PERSONNE1.) aurait indiqué à la banque que les pays de destination des virements étaient uniquement l'Allemagne, le Luxembourg et l'Autriche reste à l'état de pure allégation, PERSONNE1.) ne versant aucune pièce qui serait de nature à étayer ses dires.

La partie demanderesse prétend encore qu'elle n'aurait pas réussi à joindre la banque. Or, outre le fait que cela reste à ce stade à l'état de pure allégation, la partie demanderesse reconnaît elle-même que c'est en raison d'une longue file d'attente qu'elle n'aurait pas réussi à joindre la banque (?!). Il s'agirait donc là aussi d'une négligence grave dans le chef de la partie demanderesse, alors qu'un utilisateur normalement attentif et prudent aurait patienté.

La SOCIETE1.) aurait parfaitement respecté son obligation de vigilance puisqu'ont été bloqués les deux autres virements frauduleux de 4.500,- euros chacun.

En effet, la SOCIETE1.) disposant d'un système interne qui empêche automatiquement que plusieurs virements (et surtout à hauteur d'un même montant) soient effectués le même jour en faveur d'un bénéficiaire nouvellement créé, comme cela a été le cas en l'espèce.

Il résulterait donc de l'ensemble de ce qui précède que la partie demanderesse aurait manifestement commis des négligences graves, qui sont autant de manquements dans le chef de la partie demanderesse se trouvant à la genèse de l'accomplissement de l'opération de paiement litigieuse dont la SOCIETE1.) ne saurait partant être tenue de répondre en l'espèce.

En effet, le point (2) de l'article 88 intitulé « *La responsabilité du payeur en cas d'opérations de paiement non autorisées*» de la loi luxembourgeoise sur les services de paiement du 10 novembre 2009 dispose que : « *(2) Le payeur supporte toutes les pertes occasionnées par des opérations paiement non autorisées si ces pertes résultent d'un agissement frauduleux de sa part ou du fait que le paveur n'a pas satisfait, intentionnellement ou à la suite d'une négligence grave à une ou plusieurs des obligations qui lui incombent en vertu de l'article 83. Dans ce cas, le montant maximal visé au paragraphe (1) du présent article ne s'applique pas.* ».

Partant, la demande adverse en remboursement serait à rejeter.

Faire droit à la demande adverse aurait pour conséquence d'ouvrir grandement la porte à toutes sortes d'abus par des clients moyennement scrupuleux qui pourraient aisément, de connivence avec un soi-disant tiers, obtenir remboursement de certains de leurs virements.

PERSONNE1.) maintient l'ensemble de ses demandes formulées aux termes de la citation.

**<u>Appréciation</u> :**

Aux termes de l'article 58 du nouveau code de procédure civile, « *il incombe à chaque partie de prouver conformément à la loi les faits nécessaires au succès de sa prétention* ».

Conformément à l'article 1315 du code civil, « *celui qui réclame l'exécution d'une obligation, doit la prouver. Réciproquement, celui qui se prétend libéré, doit justifier le paiement ou le fait qui a produit l'extinction de son obligation* ».

La règle édictée aux textes susvisés régissant la charge de la preuve implique que le demandeur doit prouver les faits qui justifient sa demande et que le défendeur doit prouver les faits qui appuient ses moyens de défense.

En application des principes directeurs précités, aux fins de prospérer dans sa demande, il incombe donc à PERSONNE1.) de prouver, conformément à la loi, les actes et faits nécessaires au succès de ses prétentions.

PERSONNE1.) affirme ne pas avoir donné son consentement à l'opération ayant eu pour conséquence le virement de 9.999,- euros.

Il y a lieu de rappeler que l'article 81 de la loi du 10 novembre 2009 relative aux services de paiement, à l'activité d'établissement de monnaie électronique et au caractère définitif du règlement dans les systèmes de paiement et les systèmes de règlement des opérations sur titres dispose ce qui suit :

« *Article 81. – Le consentement et le retrait du consentement.*
*(1) Une opération de paiement n'est réputée autorisée que si le payeur a donné le consentement à l'exécution de l'opération de paiement. Une opération de paiement peut être autorisée par le payeur avant ou, si le payeur et « le » prestataire de services de paiement en ont convenu ainsi, après son exécution.*
*(2) Le consentement à l'exécution d'une opération de paiement ou d'une série d'opérations de paiement est donné sous la forme convenue entre le payeur et «le» prestataire de services de paiement. « Le consentement à l'exécution d'une opération de paiement peut aussi être donné par l'intermédiaire du bénéficiaire ou du prestataire de services d'initiation de paiement. » En l'absence « de » consentement, l'opération de paiement est réputée non autorisée.*
*(3) Le consentement peut être retiré par le payeur à tout moment, mais pas après le moment d'irrévocabilité prévue à l'article 93. Le consentement à l'exécution d'une série d'opérations de paiement peut aussi être retiré « auquel cas » toute opération de paiement postérieure « est » réputée non autorisée.*
*(4) La procédure pour donner le consentement fait l'objet d'un accord entre le payeur et « les prestataires » de services de paiement « concernés ».* »

L'article 86(2) de ladite loi dispose ce qui suit :

« *Lorsqu'un utilisateur de services de paiement nie avoir autorisé une opération de paiement qui a été exécutée, l'utilisation d'un instrument de paiement, telle qu'enregistrée par le prestataire de services de paiement, « y compris le prestataire de services d'initiation de paiement, le cas échéant, » ne suffit pas nécessairement en tant que telle à prouver que l'opération de paiement a été autorisée par le payeur ou que celui-ci a agi frauduleusement ou n'a pas satisfait, intentionnellement ou à la suite d'une négligence grave, à une ou plusieurs des obligations qui lui incombent en vertu de l'article 83. « Le prestataire de services de paiement, y compris, le cas échéant, le prestataire de services d'initiation de paiement, fournit des éléments afin de prouver la fraude ou la négligence grave commise par l'utilisateur de services de paiement.* »

Il y a lieu de se référer aux faits relatés par PERSONNE1.) lors du dépôt de sa plainte pénale le 2 mai 2025. Il en résulte que PERSONNE1.) a reçu le 23 avril 2025 un message téléphonique indiquant « annulation virement 4.500,- ». Ceci aurait été inhabituel alors que le message était rédigé en français et non pas en allemand. Il se serait connecté tout de suite via l'application SOCIETE2.) au site de la SOCIETE1.). Ce n'aurait été que par la suite qu'il se serait rendu compte que le site se terminait par « .cc » et non par « .lu ». Il aurait introduit deux à trois fois ses données personnelles. Une employée de la SOCIETE1.) l'aurait appelé pour lui demander s'il voulait effectuer un virement de 4.500,- euros. Par la suite, il aurait été informé du virement de 9.999,- euros.

Il y a lieu de constater que les faits tels que décrits par PERSONNE1.) ne sont pas précis. Le déroulement exact des faits n'est pas établi sur base de ses déclarations.

En tout état de cause, PERSONNE1.) a été victime d'une fraude ayant abouti au transfert d'un montant 9.999,- euros de son compte.

S'il est vrai que PERSONNE1.) n'avait pas l'intention de transférer le montant à une personne qui lui est inconnue, il a tout de même dû autoriser cette transaction via son dispositif SOCIETE2.), donc via une authentification forte tel qu'il résulte des données techniques fournies par la SOCIETE1.).

Aussi, il résulte des éléments soumis à l'appréciation du Tribunal, et qui ne sont en outre pas contestés par la partie demanderesse, que la transaction était subordonnée à l'authentification forte.

La SOCIETE1.) renvoie à ses conditions générales, suivant l'article 87 intitulé « *Responsabilité du client* » (pièce n°14 de la partie demanderesse) :

« *Le client doit veiller à garder strictement confidentiels tous les Codes Personnels et à ne les inscrire sur aucun document. Il s'engage à n'enregistrer que ses propres données biométriques sur son appareil dans le cadre de l'authentification via l'utilisation de données biométriques. Il s'engage en outre à respecter toutes les recommandations de l'émetteur du Moyen de Connexion, destinées à préserve la sécurité de ses Codes Personnels, de même que les principes en matière de sécurité repris sur SOCIETE1.). Il incombe exclusivement au client (i) de révéler ses Codes Personnels aux AIPS ou aux*

*PISP aux fins de la délivrance des services par ces derniers ainsi que de veiller à ce que, lorsqu'ils utilisent ces Codes Personnels, les AIPS ou PISP respectent les dispositions de la présente section VI et (ii) de choisir son mot de passe et (iii) de protéger ses Codes Personnels contre toute erreur ou imprudence.*

*Le client peut avoir accès aux services SOCIETE1.) par tout moyen adéquat quel que soit son emplacement. Afin de réduire les risques d'accès par des personnes non autorisées aux codes confidentiels d'accès du client celui-ci ne doit se connecter que directement à SOCIETE1.) et non pas indirectement p. ex. à travers des liens. Tout accès indirect par le client au site internet de la Banque se fait à ses propres risques. Internet se présente comme un réseau international ouvert, dont la structure et les spécificités sont connues du client. La Banque a pris les mesures nécessaires afin de garantir un traitement sécurisé des opérations via internet. La Banque n'assume qu'une obligation de moyens dans ce domaine* ».

Il y a lieu de souligner que PERSONNE1.) a renseigné ses données personnelles à la suite de sa connexion à un site frauduleux se terminant de ses propres déclarations par « .cc ». PERSONNE1.) a personnellement pris l'initiative, selon ses propres déclarations, de se connecter à son Internet Banking. Ce faisant il a fait confiance à un site frauduleux qui n'avait aucun lien avec la SOCIETE1.) mais qui a été spécialement mis en place pour tromper des clients de la SOCIETE1.). Le site frauduleux employé par PERSONNE1.) était cependant détectable par le client alors que PERSONNE1.), tel qu'il l'explique lui-même, a par la suite remarqué qu'il se terminait par « .cc ».

L'ensemble des données bancaires de PERSONNE1.) ont été communiquées via une authentification forte tel qu'il ressort des données techniques fournis par la SOCIETE1.). PERSONNE1.) ne nie en outre pas avoir renseigné ses données SOCIETE2.).

Il y a lieu de retenir que le fait pour PERSONNE1.) d'accéder à un site internet frauduleux, site facilement détectable alors que PERSONNE1.) déclare aux termes de sa plainte l'avoir remarqué personnellement, et de ne pas avoir respecté les recommandations d'effectuer des connexions sécurisées uniquement, est à qualifier de négligence grave requise par les dispositions de l'article 86(2) précité.

En présence de négligence grave du demandeur, la demande en remboursement formulée est à déclarer non fondée.

Pour le surplus il ne résulte d'aucun élément soumis à l'appréciation du Tribunal que la SOCIETE1.) aurait été obligé de bloquer le virement dûment autorisé ayant comme pays de destination la France.

La demande de PERSONNE1.) en remboursement du montant de 9.999,- euros ainsi que sa demande relative au préjudice moral sont partant à déclarer non fondées.

PERSONNE1.) réclame une indemnité de procédure sur base de l'article 240 du nouveau code de procédure civile.

Compte tenu de l'issue du litige, il n'y a pas lieu d'y faire droit.

Il y a finalement lieu de condamner PERSONNE1.) aux frais et dépens de l'instance.

**Par ces motifs :**

le Tribunal de Paix de et à Luxembourg, siégeant en matière civile, statuant contradictoirement et en premier ressort,

**dit** la demande recevable en la forme ;

la **dit** non fondée et en **déboute** ;

**dit** la demande de PERSONNE1.) sur base de l'article 240 du nouveau code de procédure civile non fondée et en **déboute** ;

**condamne** PERSONNE1.) aux frais et dépens de l'instance.

Ainsi fait, jugé et prononcé en audience publique par Nous, Patrice HOFFMANN, Juge de Paix, assistée de la greffière Carole HEYART, avec laquelle Nous avons signé le présent jugement, le tout, date qu'en tête.

**Patrice HOFFMANN**
**Juge de Paix**

**Carole HEYART**
**Greffière**