Texte pseudonymisé

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

Jugement civil n° 2025TALCH08/00203

Audience publique du mercredi, 3 décembre 2025.

Numéro du rôle : TAL-2025-01107

Composition :

Sandra ALVES ROUSSADO, vice-présidente,
Elodie DA COSTA, juge,
Karin SPITZ, juge,
Guy BONIFAS, greffier.

ENTRE

PERSONNE1.), sans état connu, demeurant à L-ADRESSE1.),

partie demanderesse aux termes d'un exploit de l'huissier de justice Patrick KURDYBAN de Luxembourg du 9 janvier 2025,

comparaissant par Maître Nicky STOFFEL, avocat, demeurant à Luxembourg,

ET

l'établissement public autonome SOCIETE1.) (SOCIETE1.)), établi et ayant son siège social à L-ADRESSE2.), inscrite au registre de commerce et des sociétés de Luxembourg sous le n° B NUMERO1.), représentée par le président de son comité de direction actuellement en fonctions,

partie défenderesse aux fins du prédit exploit KURDYBAN,

comparaissant par Maître Géraldine MERSCH, avocat, demeurant à Luxembourg.

LE TRIBUNAL

1. Procédure

Par exploit d'huissier du 9 janvier 2025, PERSONNE1.) (ci-après « PERSONNE1.) »), comparaissant par Maître Nicky STOFFEL, a fait donner assignation à la SOCIETE1.) (ci-après « la SOCIETE1.) ») à comparaître devant le Tribunal d'arrondissement de ce siège.

Maître Géraldine MERSCH s'est constituée pour la SOCIETE1.) en date du 17 janvier 2025.

L'affaire a été inscrite sous le numéro TAL-2025-01107 du rôle. Elle a été soumise à l'instruction de la 8e section.

Par ordonnance de mise en état simplifiée du 20 février 2025, les parties ont été informées que la procédure de la mise en état simplifiée serait applicable à la présente affaire et des délais d'instruction impartis aux parties pour notifier leurs conclusions et communiquer leurs pièces, le tout sous peine de forclusion.

Maître Géraldine MERSCH a conclu en date du 16 mai 2025 et du 15 juillet 2025, tandis que Maître Nicky STOFFEL a conclu en date du 16 juin 2025.

L'instruction a été clôturée par voie d'ordonnance du 9 septembre 2025 et l'affaire a été renvoyée à l'audience du 22 octobre 2025 pour plaidoiries.

L'affaire a été prise en délibéré à l'audience du 22 octobre 2025 par le Président de chambre.

2. Prétentions et moyens des parties

Aux termes de son exploit d'assignation, **PERSONNE1.)** demande à voir :

- dire que la SOCIETE1.) a commis une faute, sinon une négligence grave;

- condamner la SOCIETE1.) à réparer le dommage causé à PERSONNE1.);

- partant condamner la SOCIETE1.) à lui payer la somme de 35.467,92.-euros à titre de dommages et intérêts du chef des préjudices matériel et moral subis par lui, avec les intérêts légaux à partir de la demande en justice jusqu'à solde;

- condamner encore la SOCIETE1.) à lui payer des dommages et intérêts pour frais et honoraires d'avocat exposés dans le cadre du présent litige et évalué à 7.500.-euros, sur le fondement des articles 1142, 1147 et suivants du Code civil, sinon subsidiairement sur base des articles 1382, 1383 et suivants du même code;

- condamner également la SOCIETE1.) à lui payer une indemnité de procédure de 3.000.-euros sur base de l'article 240 du Nouveau Code de procédure civile;

- condamner finalement la SOCIETE1.) aux frais et dépens de l'instance, avec distraction au profit de Maître Nicky STOFFEL, qui la demande, affirmant en avoir fait l'avance.

A l'appui de sa demande, PERSONNE1.) fait valoir qu'en date du lundi, 16 février 2023 vers 10.00 heures du matin, il aurait été contacté par voie téléphonique par PERSONNE2.), employé de l'agence SOCIETE1.). Celui-ci se serait renseigné si PERSONNE1.) était bien l'auteur de virements qui auraient été effectués en date du vendredi 13 janvier 2023 en faveur de PERSONNE3.), la somme de ces virements étant de 30.000.-euros et l'argent ayant été débité du compte-courant de PERSONNE1.).

Suite à la réponse négative de PERSONNE1.) qui ignorait tout de ces virements et qui d'ailleurs ne connaîtrait pas non plus le bénéficiaire et ne serait donc forcément pas l'auteur de ces ordres de virements, celui-ci aurait demandé le blocage immédiat de son système bancaire online et aurait changé ses codes d'accès.

Lors d'une entrevue entre PERSONNE1.) et l'employé de la SOCIETE1.) postérieurement au 16 janvier 2023, il aurait eu la très mauvaise nouvelle qu'une somme supplémentaire d'environ 20.000.-euros aurait été débitée de son compte. Il se serait avéré que la banque n'avait pas procédé tout de suite au blocage des accès sur le compte de PERSONNE1.), de sorte que les virements frauduleux supplémentaires auraient pu être opérés. Ce n'est que suite à plusieurs discussions et réclamations que la banque lui aurait remboursé cette somme.

Concernant le mode opératoire mis en place dans cette affaire, il se serait avéré que PERSONNE1.) avait en date du 13 janvier 2024 vers 08.23 heures, procédé à une mise en jour de ses données informatiques relatives à son online Banking SOCIETE1.) à travers son SOCIETE2.). En effet, il aurait eu un message-texte de la part de sa banque SOCIETE1.), qui l'invitait à faire cette mise à jour en cliquant sur le lien suivant : http://oro.li/SOCIETE1.) et en se connectant par après pour terminer la mise à jour.

PERSONNE1.), en toute bonne foi, aurait fait cette mise à jour en pensant être en contact avec sa banque et de devoir faire cette mise à jour. Or, il aurait été victime d'une infraction criminelle qualifiée communément de « phishing », respectivement de « spoofing ».

Il aurait été, après avoir cliqué sur le lien indiqué dans le message-texte, orienté vers une application qu'il pensait être l'application de sa banque. Tout aurait été identique au site de la banque, l'accueil, le lay-out, la présentation de la page, les couleurs utilisées, les messages, textes et indications auraient été sans fautes d'orthographe. Aucun indice n'aurait permis à PERSONNE1.) de détecter qu'il s'agissait probablement uniquement d'une imitation frauduleuse du site de sa banque, créée par un escroc dans le but de récupérer ses informations personnelles et bancaires. Par ce biais, les données

privées de PERSONNE1.) relatives à son online-Banking et à SOCIETE2.) auraient été dérobées et par après, son compte aurait été débité à son insu, en date du 13 janvier 2023.

Il fait valoir que les sommes de 9.818.-euros, de 9.712,12.-euros, de 9.281.-euros, de 9.001,92.-euros, de 9.185.-euros et de 3.000.-euros auraient été débitées en date du 13 janvier 2023 de son compte et ce sans son autorisation.

La SOCIETE1.) lui aurait restitué les sommes de 9.818.-euros et de 9.712.12-euros et ce suite à ses réclamations. Il s'agirait là des sommes déduites de son compte après sa demande expresse de blocage.

Le préjudice subi par PERSONNE1.) se chiffrerait dès lors à 30.467,92.-euros.

Il précise que le message-texte qu'il a reçu le jour des débits, aurait indiqué comme expéditeur « *SOCIETE1.)* ». Il soutient partant qu'il aurait été envoyé par un numéro de la SOCIETE1.), du moins en apparence. L'auteur du message-texte n'aurait donc pas été une personne suspecte ou inconnue, mais bien sa banque de confiance. Il n'avait donc aucune raison de douter de l'identité de l'auteur du message.

Il soutient avoir été victime d'une cyberattaque et d'une escroquerie consistant dans le vol de l'identité électronique de sa banque en recevant un message-texte provenant de sa banque et l'invitant à dévoiler ses données personnelles d'accès à son online-Banking. Le message n'aurait contenu aucun indice permettant à un utilisateur normalement attentif de douter de sa provenance.

En droit, PERSONNE1.) estime que la SOCIETE1.) aurait commis une faute en exécutant les virements litigieux sans se renseigner immédiatement auprès de lui s'il en était vraiment l'auteur. Les virements, pris isolément, portaient sur des montants importants.

Ces virements auraient été adressés à une personne avec laquelle PERSONNE1.) n'aurait encore jamais traité. En plus, il s'agirait d'un compte que PERSONNE1.) n'utiliserait pratiquement jamais. La vigilance de la banque aurait dû être accrue dans une telle situation.

Il soutient que la banque aurait commis une faute, sinon du moins une négligence grave en exécutant ces virements sans lui demander des précisions supplémentaires et sans s'enquérir s'il était effectivement l'auteur des ordres de virement.

En outre, la banque aurait fait preuve d'une grande lenteur dans la gestion de cette situation, en ne réagissant pas directement le 16 janvier 2023, comme l'avait demandé PERSONNE1.), mais en laissant traîner les choses et en permettant ainsi à l'escroc de retirer encore pratiquement 20.000.-euros de plus sur son compte.

Malgré le fait que la banque avait découvert les agissements frauduleux qui s'opéraient sur son compte, elle n'aurait pas réagi. Ce n'est seulement suite à ses réclamations, que le montant de 20.000.-euros lui aurait été remboursé par la banque.

PERSONNE1.) soutient que quel que soit leur objet, les ordres s'analyseraient en mandats donné par le client à sa banque, pouvant s'inscrire en exécution d'une convention-cadre. Il recherche partant la responsabilité de la banque sur base des articles 1984 et suivants du Code civil.

Il soutient qu'en tant que mandataire, le banquier serait tenu d'exécuter les ordres de son client. Il devrait accomplir sa mission de manière diligente, avec le soin et la compétence attendus d'un professionnel, ainsi qu'avec loyauté au mieux des intérêts du client. Sans pouvoir s'immiscer dans les affaires de celui-ci, notamment en recherchant les raisons des opérations qu'il effectue, il devrait exécuter les ordres de son client en demeurant vigilant afin de détecter d'éventuelles anomalies apparentes affectant les ordres transmis. Il ne saurait notamment accepter sans réagir une opération manifestement irrégulière ou inhabituelle dans la pratique commerciale ou dans les habitudes du client.

En l'espèce, PERSONNE1.) soutient que la banque aurait dû réagir en voyant apparaître pas moins de six opérations de virement toujours en faveur de la même personne et toujours juste en-dessous du montant de 10.000.-euros.

Il estime que la SOCIETE1.) aurait commis une faute en exécutant les virements litigieux et en violant ainsi son obligation de vigilance née du mandat.

PERSONNE1.) se base sur l'article 87 de la loi modifiée 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 titre.

PERSONNE1.) soutient qu'il a contacté sa banque pour être indemnisé, mais celle-ci, tout en reconnaissant la survenance de l'incident, aurait refusé d'assumer la responsabilité de la fraude en alléguant qu'il n'avait pas suffisamment vérifié la sécurité du message reçu, se basant sur une présumée négligence de sa part.

PERSONNE1.) soutient qu'il a subi un préjudice matériel de 30.467,92.-euros et un préjudice moral de 5.000.-euros, soutenant avoir subi des tracasseries inutiles à cause de cette affaire. Il aurait dû se rendre chez sa banque, aurait dû constater que la banque en laquelle il avait confiance, aurait pris cette relation de confiance à la légère en ne bloquant pas immédiatement son compte et ses accès, mais en laissant faire, permettant ainsi à l'escroc de subtiliser encore 20.000.-euros.

La SOCIETE1.) demande à voir débouter PERSONNE1.) de l'intégralité de ses demandes et à le voir condamner à lui payer une indemnité de procédure de 5.000.-euros sur base de l'article 240 du Nouveau Code de procédure civile.

La SOCIETE1.) fait valoir qu'en date du 13 juillet 2022, PERSONNE1.) aurait conclu avec la SOCIETE1.) une convention d'entrée en relation d'affaires, prévoyant l'ouverture d'un compte courant.

Le même jour, PERSONNE1.) et la SOCIETE1.) auraient conclu une convention de compte courant relative au compte IBAN NUMERO2.).

La SOCIETE1.) soutient que PERSONNE1.) prétendrait désormais qu'il serait devenu victime d'une manœuvre frauduleuse en date du 13 janvier 2023 qui aurait conduit au débit de son compte d'une somme totale de 49.998,04.-euros, mais celui-ci ne verserait aucune preuve à l'appui de cette affirmation.

Il ressortirait des éléments en possession de la SOCIETE1.) qu'en date du 13 janvier 2023, PERSONNE1.) aurait franchi à trois reprises les étapes du processus d'authentification dite « *forte* », permettant l'accès au compte via SOCIETE1.), permettant l'augmentation de la limite hebdomadaire d'opérations, permettant l'ajout d'un nouveau bénéficiaire et permettant la validation des virements.

Il aurait ainsi accédé à SOCIETE1.) suite à la validation des identifiants personnels de son certificat SOCIETE2.) le 13 janvier 2023 à 8h59. Il aurait introduit son identifiant et son mot de passe SOCIETE2.), éléments que seul lui connaissait, et aurait utilisé son certificat SOCIETE2.) sur son appareil SOCIETE2.) Token, élément que lui seul possédait et qui a généré un code à usage unique.

Il aurait ensuite augmenté sa limite hebdomadaire d'opérations suite à la réintroduction des identifiants personnels de son certificat SOCIETE2.) le 13 janvier 2023 à 09h01.

Il aurait procédé à l'ajout d'un nouveau bénéficiaire suite à la validation des identifiants personnels de son certificat SOCIETE2.) le 13 janvier 2023 à 09h02.

Il aurait procédé à six transactions entre 09h03 et 09h06. Ces six virements faits depuis le compte de PERSONNE1.) au bénéfice du compte NUMERO3.) auprès de la SOCIETE1.), appartenant à PERSONNE3.), pour un montant total s'élevant à 49.998,04.-euros se décomposeraient comme suit et auraient été faits dans l'ordre chronologique suivant :

- un virement d'un montant de 9.001,92.-euros;
- un virement d'un montant de 9.281.-euros;
- un virement d'un montant de 9.818.-euros;
- un virement d'un montant de 9.712.-euros;
- un virement d'un montant de 9.185.-euros;
- un virement d'un montant de 3.000.-euros.

L'ensemble des virements aurait été ordonné le 13 janvier 2023 entre 09h03 et 09h06. Ce serait donc à tort que PERSONNE1.) semblerait faire croire qu'une somme

d'environ 20.000.-euros aurait été débitée du compte après qu'il avait prévenu la SOCIETE1.) en date du 16 janvier 2023 du fait qu'il n'était prétendument pas l'auteur des virements.

Ce serait encore à tort que PERSONNE1.) ferait soutenir que les virements à hauteur de 9.818.-euros et 9.712,12.-euros auraient été faits après sa demande expresse de blocage et que la SOCIETE1.) aurait pris cette relation de confiance à la légère en ne bloquant pas immédiatement son compte et ses accès, mais en laissant faire, permettant ainsi à l'escroc de subtiliser encore 20.000.-euros de plus de son compte.

La SOCIETE1.) soutient qu'en date du 16 janvier 2023, PERSONNE2.), employé de la SOCIETE1.), aurait contacté PERSONNE1.) par voie téléphonique à deux reprises. Cette prise de contact se serait inscrite dans un contrôle de la SOCIETE1.) relatif au compte de PERSONNE3.).

Le premier appel aurait été émis à 14h58 et non à 10h00, comme le soutiendrait PERSONNE1.). Au cours de celui-ci, PERSONNE1.) aurait déclaré qu'il n'était pas à l'origine des virements.

Au cours du second appel, émis à 15h24, PERSONNE2.) aurait indiqué à PERSONNE1.) qu'il pourrait passer à l'agence le lendemain.

Le 17 janvier 2023, la SOCIETE1.) aurait adressé six courriers à PERSONNE3.), sollicitant son consentement au retour des fonds concernés par les virements effectués, en mentionnant que la demande de remboursement se faisait suite à la demande du donneur d'ordre, PERSONNE1.).

Le 18 janvier 2023, PERSONNE1.) aurait fait une déclaration de vol en ligne via le site de la Police Grand-Ducale, dans le cadre de laquelle, il aurait déclaré ce qui suit :

« J'ai été victime d'un piratage de données de mon compte bancaire. La transaction frauduleuse s'est déroulée avec les applications en ligne « S-net » de la Spuerkees et SOCIETE2.). Suite à ce piratage une somme de 54.574,45 € (cinquante-quatre-mille-cinque-cents-soixante-quatorze € et quarante-cinq centimes) a été dévié sur le compte bancaire d'une Madame PERSONNE3.). Cette dame m'est complètement inconnue. 6 transactions frauduleuses ont été effectuées pour arriver à la somme finale de 54.574,45 €. La Spuerkees m'a obligé de porter plainte pour que le dossier puisse être traité par leur « bureau des fraudes ».

Il y aurait lieu de s'interroger sur la somme de 54.574,45.-euros citée par PERSONNE1.), alors que la somme des virements ne s'élèverait qu'à 49.998,04.-euros.

Le 8 février 2023, la SOCIETE1.) aurait adressé 4 courriers à PERSONNE1.) pour l'informer que ses demandes en remboursement concernant les paiements à hauteur de 9.818.-euros, de 9.712,12.-euros, de 9.281.-euros et de 9.001,92.-euros étaient restées sans succès.

En date du 3 mars 2023, PERSONNE3.) aurait notifié son accord uniquement quant au remboursement des paiements à hauteur de 9.818.-euros et de 9.712,12.-euros à la SOCIETE1.).

Ainsi, la SOCIETE1.) aurait procédé le 6 mars 2023 à la restitution des montant de 9.818.-euros et 9.712,12.-euros à PERSONNE1.).

Le 16 mars 2023, la SOCIETE1.) aurait adressé un courrier à PERSONNE1.) pour l'informer que sa demande en remboursement concernant le paiement à hauteur de 3.000.-euros était restée sans succès pour solde insuffisant du compte de PERSONNE3.).

Le 28 mars 2023, la SOCIETE1.) aurait adressé un courrier à PERSONNE1.) pour l'informer que sa demande en remboursement concernant le paiement à hauteur de 9.185.-euros était restée sans succès.

Le 30 août 2023, le mandataire de PERSONNE1.) aurait demandé le remboursement du montant de 30.467,92.-euros à la SOCIETE1.) en précisant que PERSONNE1.) n'aurait commis aucune négligence grave, de sorte que les articles 27 et 38 des conditions générales de la SOCIETE1.) ne s'appliqueraient pas.

Par courrier du 26 septembre 2023, la SOCIETE1.) l'aurait informé qu'elle ne pouvait accéder à cette demande, en exposant que les virements étaient à qualifier d'opérations autorisées au sens 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 règlement des opérations sur titres.

Le 26 juillet 2024, c'est-à-dire presqu'un an après le courrier de la SOCIETE1.), le mandataire de PERSONNE1.) aurait renouvelé sa demande de remboursement de la somme de 30.467,92.-euros, son courrier mentionnant que *« mon client a répondu à un message provenant de la société SOCIETE2.). »*

Pourtant, aux termes de son assignation, PERSONNE1.) indiquerait qu'il *« avait un message-texte de la part de sa banque Spuerkees, qui l'invitait à faire cette mise à jour en cliquant sur le lien indiqué http://oro.li/Spuerkees et en se connectant par après pour terminer la mise à jour. »*

PERSONNE1.) se contredirait donc en ce qu'il aurait, dans une première phase, affirmé qu'il aurait reçu un message, dont la nature exacte demeurerait inconnue, de la part de SOCIETE2.) et puis, dans une deuxième phase, qu'il aurait reçu un message-texte, supposément un SMS, de la part de la SOCIETE1.). Or, ni l'un ni l'autre de ses deux récits ne pourrait être vérifié à défaut d'une quelconque pièce à ce sujet. PERSONNE1.) resterait en défaut de verser en pièce le prétendu message-texte, une capture d'écran du prétendu site frauduleux ou une quelconque pièce relative à la prétendue fraude dont il serait devenu victime.

Au-delà de l'incohérence entre ces deux récits, il y aurait lieu d'apporter quelques commentaires quant au récit de PERSONNE1.) de la prétendue fraude aux termes de l'assignation du 9 janvier 2025.

Premièrement, PERSONNE1.) prétendrait que le message-texte lui serait parvenu depuis un numéro de la SOCIETE1.), *« du moins en apparence »*, sans pour autant préciser le numéro. A défaut d'une quelconque pièce concernant ce message, cette affirmation resterait à l'état de pure allégation.

Deuxièmement, le lien http://oro.li/Spuerkees ne donnerait aujourd'hui aucun résultat de recherche.

Le lien serait douteux, contrairement à ce que ferait affirmer PERSONNE1.) à plusieurs titres :

- le lien prétendument communiqué à PERSONNE1.) ferait référence au protocole http (hypertext transfer protocol) au lieu du protocole http (hypertext transfer protocole secure). La SOCIETE1.) rappelle que l'article 25.4 des conditions générales de la SOCIETE1.) préciserait que le client doit s'assurer de la présence du certificat digital du server de la SOCIETE1.) dans son navigateur. L'échange entre l'outil électronique du client et la serveur SOCIETE5.) serait sécurisé par un mécanisme de chiffrement visible via le début d'adresse https;

- le domaine donnant accès au système bancaire en ligne SOCIETE1.) de la SOCIETE1.) serait le suivant : bcee.snet.lu.. En l'espèce, PERSONNE1.) prétendrait qu'un lien oro.li n'aurait rien de suspect, alors qu'il ne comprendrait ni le mot SOCIETE1.) ni l'extension du Grand-Duché. Au contraire, ce domaine comporterait l'extension nationale du pays de Liechtenstein. A suivre les développements de PERSONNE1.), cet élément n'aurait eu rien de douteux pour lui.

Troisièmement, PERSONNE1.) resterait en défaut d'exposer les démarches exactes qu'il a faites. Il prétendrait avoir procédé à une mise à jour de ses données informatiques relatives à son online Banking SOCIETE1.) à travers son Token SOCIETE2.), mais ne préciserait pas la nature des informations qu'il aurait introduites sur ce prétendu site frauduleux.

Quatrièmement, PERSONNE1.) ne préciserait pas non plus à quel moment il lui aurait été demandé de s'authentifier avec ses identifiants SOCIETE2.). Il affirmerait juste qu'il a dû se connecter par après pour terminer la mise à jour. Tout porterait donc à croire que PERSONNE1.) a introduit des informations confidentielles, dont la nature demeure inconnue, sur un site ressemblant prétendument à celui de la SOCIETE1.), sans devoir s'authentifier. Cet élément n'aurait donc pas non plus alerté PERSONNE1.).

Par courrier du 22 août 2024, la SOCIETE1.) aurait réitéré son refus de rembourser à PERSONNE1.) le montant réclamé.

La SOCIETE1.) précise de manière générale que face à la recrudescence des escroqueries et manœuvres frauduleuses, telles que le phishing, elle publierait depuis quelques années et continuerait à publier sur son site Internet et notamment lors de la connexion à SOCIETE1.) une alerte exhortant ses clients à faire preuve d'une vigilance accrue.

En droit, la SOCIETE1.) entend d'abord prendre position quant à la loi sur les services de paiement dans la mesure où elle estime que l'application de cette loi exclurait tout autre fondement de la responsabilité.

Elle soutient que la prédite loi mettrait en place un régime spécial de responsabilité du prestataire de services de paiement en cas d'opérations de paiement non autorisées.

S'agissant de l'article 87 de la prédite loi sur laquelle se base PERSONNE1.), le prédit régime ne s'appliquerait qu'en présence de paiements non autorisés au sens de la loi sur les services de paiement.

Or, le payeur supporterait toutes les pertes occasionnées par des opérations de paiement non autorisées dans certaines hypothèses conformément à l'article 88 de la loi sur les services de paiement relatif à la responsabilité du payeur en cas d'opérations de paiement non autorisées qui disposerait en son point (2) 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 payer 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. »*

L'article 83 de la loi sur les services de paiement énoncerait par ailleurs certaines obligations dans le chef du payeur :

« (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 des données de sécurité personnalisées. »

En l'espèce, le régime de responsabilité mis en place par l'article 87 de la loi sur les services de paiement ne s'appliquerait pas à défaut d'opération non autorisée et pour autant que ce régime s'applique, PERSONNE1.) supporterait seul la perte occasionnée par les virements au vu de la négligence grave commise en son chef.

La SOCIETE1.) estime que les virements étaient des opérations autorisées par PERSONNE1.), au sens de la loi sur les services de paiement.

Elle soutient que l'élément déclencheur du régime de responsabilité mis en place par l'article 87 de la loi sur les services de paiement consisterait dans la survenance d'une opération non autorisée. Autrement dit, ce régime ne s'appliquerait pas à défaut d'opération non autorisée.

L'article 81 de la loi sur les services de paiement disposerait ce qui suit :

« (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.

(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'opération de paiement serait présumée autorisée, au sens de la loi sur les services de paiement, lorsqu'il y a un consentement dans le chef du payeur dans le sens objectif du terme. Il faudrait, mais il suffirait que le consentement ait été donné sous la forme convenue entre le payeur et le prestataire de services de paiement. Ainsi, la notion d'autorisation au sens de la loi sur les services de paiement, serait étrangère à l'intention réelle du payeur.

Il faudrait, mais il suffirait que le consentement ait été donné selon la forme convenue entre parties.

Quant à la charge de la preuve de l'opération non autorisée, il incomberait au client de prouver son caractère non autorisé lorsque le prestataire de services de paiement a prouvé que l'opération en question a été authentifiée, dûment enregistrée et comptabilisée, conformément à l'article 86 de la loi sur les services de paiement.

La SOCIETE1.) rappelle encore que l'article 30.1 des conditions générales de la SOCIETE1.) disposerait que toute opération effectuée par l'intermédiaire de SOCIETE1.) moyennant l'utilisation des éléments d'identification SOCIETE2.) est réputée émaner de ce dernier.

Aux termes de son article 30.3, le client autoriserait la SOCIETE1.) à rapporter la preuve de son consentement à la réalisation de l'opération par la circonstance que le procédé de validation ait été validé par le client,

En l'espèce, la SOCIETE1.) soutient que les virements litigieux auraient été autorisés par PERSONNE1.). Ils ne seraient pas à qualifier d'opérations non autorisées au sens de la loi sur les services de paiement.

En effet, PERSONNE1.) se serait connecté à SOCIETE1.) moyennant les identifiants de son certificat SOCIETE2.) et le mot de passe unique généré par son Token.

L'augmentation de la limite hebdomadaire des opérations aurait également exigé une authentification forte de la part de PERSONNE1.) moyennant son certificat SOCIETE2.).

L'ajout d'un nouveau bénéficiaire aurait également exigé une authentification forte de la part de PERSONNE1.) moyennant son certificat SOCIETE2.).

PERSONNE1.) aurait ensuite validé les virements.

Les virements auraient été ordonnés et exécutés selon la procédure convenue entre la SOCIETE1.) et PERSONNE1.) conformément à l'article 30.1 des conditions générales de la SOCIETE1.). La SOCIETE1.) estime avoir rapporté la preuve de son consentement conformément à l'article 30.3 des conditions générales.

PERSONNE1.) n'aurait d'ailleurs jamais contesté et ne contesterait toujours pas que les virements aient été ordonnés et exécutés selon la procédure convenue entre lui-même et la SOCIETE1.).

PERSONNE1.) n'allèguerait d'ailleurs aucune déficience technique.

Les virements auraient ainsi été autorisés au sens de la loi sur les services de paiement et n'auraient pas fait l'objet d'une déficience technique. La charge de la preuve du caractère non autorisé des virements reviendrait donc à PERSONNE1.).

Dans ce contexte, la SOCIETE1.) conteste que PERSONNE1.) soit devenu victime d'une quelconque manœuvre frauduleuse à défaut d'une quelconque pièce à l'appui de son récit des faits et surtout au vu des contradictions dans les différents récits faits par PERSONNE1.).

Même à supposer que les faits se soient déroulés comme décrits par PERSONNE1.) dans l'assignation, les virements seraient à qualifier d'opérations de paiement autorisées au sens de la loi sur les services de paiement dans la mesure où la notion d'autorisation au sens de cette loi serait étrangère à la question de l'intention réelle du payeur.

Au vu de ce qui précède, à défaut pour les virements d'être qualifiés d'opérations non autorisées au sens de la loi sur les services de paiement, le régime de responsabilité mis en place par l'article 87 de la loi sur les services de paiements ne s'appliquerait pas au cas d'espèce.

Même à supposer que le régime de responsabilité mis en place par l'article 87 de la loi précitée s'applique au cas d'espèce étant donné que les virements seraient à qualifier d'opérations de paiement non autorisées, PERSONNE1.) devrait supporter les pertes occasionnées par les virements, dans la mesure où il aurait commis une négligence grave au sens de l'article 88 (2) de la loi précitée.

En effet, la négligence grave du client de la banque exclurait la responsabilité de la banque sur base de l'article 87 de la loi précitée.

La Cour de cassation française apprécierait la négligence grave en fonction de la manœuvre frauduleuse à laquelle a concrètement été confrontée le client de la banque.

En l'espèce, PERSONNE1.) aurait commis une négligence grave au sens de l'article 88 (2) de la loi sur les services de paiement à plusieurs titres :

- PERSONNE1.) ne se serait pas étonné que la SOCIETE1.) lui demande, à travers un *« message-texte »* de mettre à jour des informations via un site qui n'aurait rien de commun avec son domaine et qu'elle ne lui adresse pas la demande à travers la messagerie sécurisée sur SOCIETE1.). Le comportement de PERSONNE1.) serait aussi à analyser à la lumière de l'article 27.1. des conditions générales de la SOCIETE1.) qui préciserait que la SOCIETE1.) ne demande jamais à son client de se connecter à SOCIETE1.) moyennant un lien. Il aurait ensuite cliqué sur un lien dont le domaine ne correspondrait pas à celui de la SOCIETE1.) et dont l'extension du pays correspondrait non pas à celle du Grand-Duché de Luxembourg, mais à celle du Liechtenstein;

- La SOCIETE1.) aurait établi, moyennant les pièces fournies, que les virements ont été ordonnés suite à 3 authentifications fortes par PERSONNE1.) moyennant ses identifiants personnels SOCIETE2.). PERSONNE1.) aurait nécessairement dû fournir ces éléments, dont le mot de passe à usage unique généré par son Token, à trois différentes reprises. L'authentification « *forte* » à 3 reprises

moyennant ses identifiants SOCIETE2.) aux seules fins de modifier ses informations auraient dû alerter PERSONNE1.).

Même à supposer que les faits se soient déroulés comme décrits par PERSONNE1.) aux termes de son assignation, la fraude dont il prétend être devenu victime aurait été opérée par écrit. Contrairement à la victime d'une fraude par téléphone, il disposait du temps nécessaire pour s'apercevoir des anomalies révélatrices de la prétendue fraude et, le cas échéant, appeler la SOCIETE1.) pour confirmer la démarche.

Or, il aurait choisi de suivre aveuglement les instructions qui lui ont été prétendument communiquées sans aucune remise en question malgré des anomalies apparentes, révélatrices de la prétendue fraude.

Il y aurait partant lieu de débouter PERSONNE1.) de sa demande, en ce qu'elle serait fondée sur l'article 87 de la loi sur les services de paiement.

Quant à la demande de PERSONNE1.) basée sur l'articles 1984 et suivants du Code civil, la SOCIETE1.) soutient que sa responsabilité ne pourrait être analysée à la lumière de ces articles, dans la mesure où la loi sur les services de paiement s'appliquerait aux virements. En effet, lorsque la responsabilité d'un prestataire de services de paiement est recherchée sur base d'une opération prétendument non autorisée ou mal exécutée, seul serait applicable le régime de responsabilité issu de la loi sur les services de paiement, à l'exclusion de tout régime alternatif de responsabilité résultant du droit national.

En tout état de cause, elle soutient n'avoir commis aucune violation de son devoir de vigilance.

En effet, les virements n'auraient présenté aucune anomalie apparente qui ne devrait pas échapper à un banquier normalement vigilant, car PERSONNE1.) se serait identifié à SOCIETE1.) moyennant une authentification forte grâce à ses identifiants personnels SOCIETE2.). Il aurait ensuite augmenté sa limite hebdomadaire d'opérations et aurait rajouté PERSONNE3.) comme bénéficiaire. Il aurait finalement encodé les virements et les aurait validés.

PERSONNE1.) resterait en défaut d'exposer en quoi le comportement de la SOCIETE1.) n'aurait pas correspondu au comportement de toute autre banque normalement prudente et diligente placée dans la même situation. Or, dans la mesure où le devoir de vigilance serait une obligation de moyens, il appartiendrait à PERSONNE1.) de prouver une faute dans le chef de la SOCIETE1.), ce qu'il ne ferait pas.

De plus, PERSONNE1.) n'établirait ses habitudes ni quant à la gestion du compte en particulier, ni dans ses relations avec la SOCIETE1.) de manière générale. Aucun élément dans les pièces de PERSONNE1.) ne permettrait de conclure que les virements étaient à qualifier d'inhabituels au regard de ses habitudes.

La SOCIETE1.) fait valoir que la subdivision en plusieurs opérations pourrait être parfaitement justifiée, notamment aux fins de distinguer entre plusieurs causes de paiement. Elle soutient qu'elle n'aurait pas à s'immiscer dans la manière dont le client opère ses virements.

Même à supposer que la SOCIETE1.) ait violé son devoir de vigilance, PERSONNE1.) n'aurait subi aucun préjudice en lien causal avec cette prétendue violation.

En effet, le préjudice allégué par PERSONNE1.) aurait été causé par les instructions de virements faites moyennant les identifiants SOCIETE2.) de PERSONNE1.). La SOCIETE1.) se serait limitée à exécuter les ordres de virements qu'elle aurait reçu, conformément à ses obligations contractuelles vis-à-vis de PERSONNE1.).

De plus, s'agissant du préjudice moral réclamé qui est contesté, celle-ci fait valoir que PERSONNE1.) serait toujours client de la SOCIETE1.), de sorte que sa relation de confiance avec sa banque n'aurait visiblement pas été rompu. La SOCIETE1.) n'aurait pas pris la situation de PERSONNE1.) à la légère.

La SOCIETE1.) conteste également les frais et honoraires d'avocats réclamés à défaut d'une quelconque pièce relativement aux honoraires concrètement facturés et relative à la preuve de paiement de ces honoraires, tout comme elle conteste l'indemnité de procédure réclamée.

Elle réclame à son tour la condamnation de PERSONNE1.) à lui payer une indemnité de procédure de 5.000.-euros sur base de l'article 240 du Nouveau Code de procédure civile.

PERSONNE1.) soutient avoir reçu un appel téléphonique, ainsi que plusieurs communications électroniques d'individus usurpant l'identité visuelle et institutionnelle de son établissement bancaire.

Il verse une capture d'écran du message-texte dont il a fait état et soutient qu'il s'agissait bien d'un message de la part de la SOCIETE1.) tel que décrit dans l'assignation.

Il soutient que sous le couvert d'une prétendue urgence liée à la sécurité de son compte bancaire, il lui aurait été demandé de confirmer certaines opérations et de transmettre des codes d'authentification pour prétendument sécuriser ses accès.

Contrairement à ce que prétendrait la SOCIETE1.), PERSONNE1.) conteste avoir agi avec légèreté ou imprudence, soutenant s'être trouvé confronté à un stratagème frauduleux particulièrement élaboré, usurpant de manière crédible l'identité de la SOCIETE1.). L'apparence du numéro d'appel, la présentation du message, l'usage du protocole sécurisé « *https* », le logo officiel de la banque, ainsi que le ton institutionnel de la communication auraient tous été soigneusement conçus pour induire en erreur un client raisonnablement attentif.

Il prétend qu'à son insu, ces actions auraient en réalité permis aux fraudeurs d'augmenter d'abord la limite hebdomadaire d'opérations, d'ajouter un nouveau bénéficiaire et d'initier une série de virements frauduleux depuis son compte.

Ce serait donc à tort que la SOCIETE1.) soutiendrait que les virements litigieux auraient été autorisés par PERSONNE1.) et qu'il les aurait par la suite validés. En effet, l'autorisation alléguée par la SOCIETE1.) reposerait sur des données d'identification et des codes d'authentification que PERSONNE1.) aurait transmis sous la contrainte d'un stratagème frauduleux particulièrement sophistiqué, dans un contexte d'urgence artificiellement créé par les fraudeurs, se faisant passer pour sa banque.

La prétendue autorisation donnée par PERSONNE1.) ne saurait dès lors être considérée comme un consentement valable au sens juridique, dans la mesure où elle aurait été extorquée par tromperie, usurpation d'identité et manipulation psychologique.

En outre, conformément à la directive (UE) 2015/2366 relative aux services de paiement, transposée en droit luxembourgeois, la charge de la preuve de l'authentification, de l'exécution correcte et de l'absence de défaillance technique ou de faille de sécurité incomberait à la SOCIETE1.).

Il soutient par conséquent que les virements litigieux n'auraient pas été valablement autorisés et que la responsabilité de leur exécution frauduleuse ne saurait lui être imputée, mais relèverait d'un manque au devoir de sécurité et de vigilance de la part de la SOCIETE1.).

PERSONNE1.) conteste formellement que les virements litigieux aient été ordonnés et exécutés conformément à la procédure contractuelle convenue entre lui-même et la SOCIETE1.).

Il soutient ne jamais avoir initié lesdits virements depuis l'interface bancaire sécurisée mise à disposition par la SOCIETE1.), dans le respect des étapes et formalités prévues à cet effet, que les éléments d'authentification utilisés auraient été obtenus frauduleusement, en dehors de tout cadre contractuel, dans le contexte d'une escroquerie reposant sur l'usurpation de l'identité de la SOCIETE1.) et que la validation de l'opération n'aurait pas été opérée conformément aux protocoles normalement requis par la SOCIETE1.).

Il soutient par ailleurs que la SOCIETE1.), en sa qualité d'établissement bancaire, serait tenue à une obligation de moyens renforcée en matière de sécurité informatique et de protection contre les fraudes, impliquant notamment la détection des opérations anormales ou inhabituelles, ainsi que la mise en œuvre de systèmes d'alerte ou de blocage automatique en cas de comportement suspect. En ne parvenant pas à détecter une utilisation frauduleuse des accès de PERSONNE1.), elle aurait failli à ses obligations contractuelles et réglementaires.

Il fait valoir que les débits auraient été effectués le 13 janvier 2023 et que ce n'est que le 16 janvier 2023 que la banque l'aurait contacté pour s'enquérir du fait s'il était bien à l'origine de ces virements. La banque avait donc bien conscience que les opérations effectuées étaient frauduleuses ou du moins inhabituelles.

Il soutient ne jamais avoir auparavant fait un virement en faveur de PERSONNE3.), son argent étant parti au Portugal, pays avec lequel il n'aurait aucune relation. De plus, les montants virés seraient particulièrement élevés, contrairement à ses habitudes, les opérations bancaires étant généralement effectuées pour des montants faibles. Tous ces indices auraient dû mettre en vigueur un système d'alerte auprès de la banque au lieu d'attendre trois jours avant de le contacter.

Dès qu'il aurait pris connaissance de ces débits anormaux le 16 janvier 2023 au matin, PERSONNE1.) aurait immédiatement demandé à la SOCIETE1.) de procéder au blocage de son compte et de tenter de récupérer les fonds indûment transférés. Il aurait insisté sur le fait qu'il n'avait en aucune manière validé ces virements en connaissance de cause, mais qu'il avait été victime d'un stratagème usurpant l'identité de la banque.

Cependant, la réaction de la SOCIETE1.) aurait été tardive et insuffisante. Aucune opposition efficace n'aurait pu empêcher l'exécution complète des ordres frauduleux déjà initiés et les tentatives pour faire rapatrier les sommes versées à l'étranger se seraient révélées infructueuses. Cette lenteur et ce défaut de vigilance de la part de la SOCIETE1.), auraient directement contribué à la réalisation du préjudice subi.

S'agissant de l'application de la loi du 10 novembre 2009, PERSONNE1.) conteste avoir commis une négligence grave. Il estime que la SOCIETE1.) resterait en défaut de prouver la moindre faute lourde dans son chef. Il soutient qu'au contraire, les éléments du dossier le dépeigneraient comme la victime de manœuvres particulièrement trompeuses auxquelles n'importe quel usage prudent pourrait se laisser prendre.

Il fait valoir que les malfaiteurs auraient eu recours au *« spoofing »*, c'est-à-dire à l'usurpation de l'identité de la banque, en affichant notamment sur son téléphone le numéro officiel de son agence bancaire. Ils auraient reproduit le ton et le contenu de communications bancaire légitimes.

Ce contexte de confiance artificiellement créé aurait fortement diminué la vigilance de PERSONNE1.) en le convainquant qu'il communiquait réellement avec un employé de la SOCIETE1.).

Il souligne qu'il avait déjà eu quelques semaines avant le 13 janvier 2023 des soucis avec sa connexion SOCIETE2.) qui étaient régulièrement perturbée en raison de coupures temporaires comme si des informaticiens SOCIETE2.) travaillaient sur leur système. Le message reçu par la SOCIETE1.) n'aurait donc pas été étonnant pour PERSONNE1.). Il pensait que cette réinitialisation allait définitivement résoudre les problèmes de connexion antérieurs.

Il soutient n'avoir communiqué aucune information que la SOCIETE1.) elle-même ne demande habituellement à ses clients dans le cadre de ses procédures de sécurité. En effet, les codes transmis étaient ceux générés par le dispositif SOCIETE2.) qu'il utiliserait pour authentifier ses opérations bancaires. Il soutient avoir cru de bonne foi suivre une procédure de vérification initiée par son établissement.

Son erreur constituerait tout au plus une imprudence légère.

Il conteste le fait que la SOCIETE1.) ne contacterait pas ses clients par SMS et verse plusieurs captures d'écran montrant que la SOCIETE1.) le contactait régulièrement par SMS et toujours avec le même numéro. Il soutient donc avoir reçu des messages authentiques de sa banque de la part de ce même numéro que celui utilisé par les malfaiteurs.

Il demande partant, en application des articles 85 et 87 de la loi du 10 novembre 2009 d'être replacé dans la situation où se trouverait son compte bancaire si les virements frauduleux n'avaient pas eu lieu, dès lors qu'il n'aurait jamais consenti à ces paiements.

La SOCIETE1.) soutient que PERSONNE1.) ne saurait valablement soutenir qu'il n'a jamais initié lesdits virements depuis l'interface bancaire sécurisée mise à sa disposition par la SOCIETE1.), dans le respect des étapes et formalités prévues à cet effet. Il admettrait en effet avoir communiqué les éléments d'authentification forte.

Il reconnaîtrait également que la SOCIETE1.) aurait bien mis en œuvre un système d'authentification à deux facteurs.

Elle soutient encore que PERSONNE1.) exposerait, dans le cadre de ses conclusions une nouvelle version des faits. Il affirmerait en effet avoir été contacte par téléphone le 13 janvier 2023, sans toutefois en apporter la moindre justification. Il ferait référence à l'apparence du numéro légitime de la SOCIETE1.) ou de l'appel téléphonique provenant de la banque, sans fournir d'élément concret à l'appui de ses affirmations, ne serait-ce que de mentionner le prétendu numéro en question.

Par ailleurs, il ne préciserait ni le contenu de l'échange téléphonique, ni les instructions qui lui auraient prétendument été données au cours de cet appel. Aucune pièce ne serait fournie à l'appui de l'existence de ce prétendu entretien.

De plus, PERSONNE1.) produirait désormais les messages qu'il aurait prétendument reçus de la SOCIETE1.) le 13 janvier 2023. Or, ni l'année, ni le numéro de téléphone de l'expéditeur ne figureraient sur la capture d'écran versée aux débats, de sorte qu'il ne serait même pas établi que le message en question ait été envoyé le 13 janvier 2023, comme le soutiendrait PERSONNE1.).

De plus, il ne serait plus question d'un seul message mais de deux SMS reçus prétendument en date du 13 janvier 2023 de la part de la SOCIETE1.), envoyés sous deux noms de contacts différents, à savoir « SOCIETE1.) » et « spuerkees », l'invitant

à procéder à la mise à jour de son Token SOCIETE2.), en plus d'un appel téléphonique prétendument émis par la SOCIETE1.).

Au-delà de l'incohérence entre les différentes versions du déroulement proposées par PERSONNE1.), quelques commentaires s'imposeraient :

- s'agissant des deux messages prétendument reçus, ils seraient au nombre de un et non deux, ne comporteraient aucun numéro d'expéditeur identifiable, mais seulement deux noms de contact distincts. Le numéro utilisé ne pourrait être vérifié. PERSONNE1.) prétendrait ne pas s'être étonné que deux messages identiques lui soient envoyés de la part de deux expéditeurs différents. De même, le soi-disant appel téléphonique qu'il aurait reçu de la SOCIETE1.) ne serait étayé par aucune pièce;
- le lien http://oro.li/Spuerkees dont fait état PERSONNE1.) dans le cadre de son assignation ne donnerait aujourd'hui aucun résultat de recherche. Aux termes de ses conclusions, la capture d'écran montrerait le lien https://oro.li/Spuerkees, ce qui montrerait encore une fois une modification de la version des faits de PERSONNE1.). De plus, ce lien ne donnerait également aucun résultat de recherche.

  Le prédit lien serait douteux, contrairement à ce qu'affirmerait PERSONNE1.), le domaine donnant accès au système bancaire en ligne SOCIETE1.) de la SOCIETE1.) étant bcee.snet.lu.

  Par conséquent le lien communiqué aux termes des messages reçus par PERSONNE1.) aurait présenté des anomalies apparentes, mais en plus le mode de réception de ces messages aurait présenté des anomalies dans la mesure où ils émanaient de deux expéditeurs différents, dont le numéro de téléphone ne s'afficherait pour aucune.

- PERSONNE1.) resterait en défaut d'exposer les démarches exactes qu'il a faites. Il prétend avoir procédé à une mise à jour des données informatiques relatives à son online- Banking SOCIETE1.) à travers son Token SOCIETE2.), mais ne préciserait pas la nature des informations qu'il aurait introduites sur ce prétendu site frauduleux. Il affirmerait désormais avoir agi sous le couvert d'une prétendue urgence liée à la sécurité de son compte bancaire. Dans ce contexte, il confirmerait avoir transmis ses codes d'authentification pour sécuriser ses accès.

  Or, il ne produirait aucune pièce à l'appui de ses allégations, de sorte qu'il serait impossible de comprendre et d'établir comment il lui aurait été demandé de confirmer ces opérations et de transmettre ses codes d'authentification. Il ferait état du lien prétendument frauduleux sans toutefois préciser ce qui lui aurait été demandé de faire.

  Il admettrait avoir confirmé certaines opérations et transmis ses codes d'authentification.

PERSONNE1.) soutiendrait que les messages reçus le 13 janvier 2023, émanant prétendument de la SOCIETE1.), avaient un lien avec la mise à jour ou la sécurité de sa convention SOCIETE1.).

Pourtant, l'analyse des messages précités montrerait qu'il lui aurait été demandé de faire une mise à jour de son Token SOCIETE2.), sans aucune référence à sa convention SOCIETE1.).

Or, la société SOCIETE2.) serait indépendante de la SOCIETE1.).

La mise à jour d'un Token SOCIETE2.) ne ferait aucun sens dans la mesure où cet appareil ne requérait pas de mise à jour. Il s'agirait d'un appareil qui n'avait d'autre fonction que de générer un code à usage unique à six chiffres.

Les certificats SOCIETE2.) et non les dispositifs permettant d'y accéder, tels que le Token, pourraient faire l'objet d'une procédure de renouvellement après leur expiration, et non pas d'une mise à jour, comme cela serait mentionné dans les messages frauduleux reçus par PERSONNE1.). Le certificat SOCIETE2.) expirerait après 3 ans. Cette procédure serait spécifique et hautement sécurisée, ses étapes étant clairement détaillées sur le site officiel de SOCIETE2.).

La SOCIETE1.) n'interviendrait à aucun moment dans la gestion, la délivrance ou le renouvellement des certificats électroniques émis par SOCIETE2.), prestataire indépendant.

De plus, lorsqu'un utilisateur accèderait au site officiel de SOCIETE2.), un message d'alerte exhorterait les utilisateurs à faire preuve de vigilance face à la multiplication des escroqueries.

- PERSONNE1.) ne préciserait pas non plus à quel moment il lui aurait été demandé de s'authentifier avec ses identifiants SOCIETE2.). Il affirmerait juste qu'il a dû se connecter par après pour terminer la mise à jour. Tout porterait donc à croire que PERSONNE1.) aurait introduit des informations confidentielles, dont la nature demeurerait inconnue, sur un site ressemblant prétendument à celui de la SOCIETE1.) sans devoir d'abord s'authentifier avec son certificat SOCIETE2.). Cet élément n'aurait donc pas non plus alerté PERSONNE1.).

En droit, la SOCIETE1.) fait valoir que l'article 88 (a) de la loi sur les services de paiement concernerait les pertes liées à toute opération de paiement non consécutive à l'utilisation d'un instrument de paiement perdu ou volé ou au détournement d'un instrument de paiement. Cet article mettrait en place un montant maximal de perte à supporter par le client à hauteur de 50.-euros. Conformément à la dernière phrase de l'article 88 (2) de la même loi, le prédit montant maximal ne s'appliquerait pas lorsque le client n'a pas respecté ses obligations en vertu de l'article 83 suite à une négligence grave.

S’agissant de la charge de la preuve de l’opération non autorisée, la SOCIETE1.) fait valoir avoir fourni les pièces probantes quant à l’authentification forte de PERSONNE1.). Mais en plus, PERSONNE1.) serait lui-même en aveu d’avoir fourni les éléments d’authentification forte.

Les pièces versées par la SOCIETE1.) démontreraient que les trois processus d’authentification forte n’auraient fait l’objet d’aucune déficience technique.

Par conséquent, l’authentification forte par PERSONNE1.) moyennant son certificat SOCIETE2.) serait établie et la charge de la preuve du prétendu caractère non autorisé des virements reviendrait à PERSONNE1.).

Quant à l’absence d’opération non autorisée en l’espèce, PERSONNE1.) contesterait désormais que les virements ont été ordonnés et exécutés selon la procédure convenue entre lui-même et la SOCIETE1.), sans toutefois préciser ni identifier les dispositions contractuelles prétendument violées.

Pourtant, il soutiendrait que la SOCIETE1.) a bien mis en œuvre un système d’authentification à 2 facteurs, soit un système d’authentification forte.

Les virements n’auraient été affectés d’aucune déficience technique et PERSONNE1.) n’allèguerait d’ailleurs aucune déficience technique.

Les virements auraient ainsi été autorisés au sens de la loi sur les services de paiement, dans la mesure où ils ont fait suite à une authentification forte par PERSONNE1.) et dans la mesure où ils n’ont pas fait l’objet d’une déficience technique.

De plus, la SOCIETE1.) estime que PERSONNE1.) a commis une négligence grave au sens de l’article 88 (2) de la loi sur les services de paiement à plusieurs titres :

- il prétendrait avoir cliqué sur un lien qui lui aurait été envoyé par un message-texte. Il aurait affirmé dans une première phase que ce message lui serait parvenu de SOCIETE2.) et il aurait affirmé dans une deuxième phase que ce message lui serait parvenu de la part de la SOCIETE1.), l’invitant à procéder à une mise à jour de ses données informatiques relatives à son online Banking SOCIETE1.) à travers son Token SOCIETE2.). Dans aucune de ses deux versions du déroulement des faits, il n’aurait mentionné un numéro de téléphone de l’expéditeur;

- PERSONNE1.) ferait désormais produire plusieurs captures d’écran de messages qu’il aurait prétendument reçus de la SOCIETE1.), dans lesquels le nom de l’expéditeur apparaîtrait sous les intitulés « SOCIETE1.) » et « spuerkees », l’invitant à mettre à jour son Token SOCIETE2.) via une adresse URL particulièrement douteuse qui ne comprend pas le nom de domaine utilisé par la SOCIETE1.) pour l’accès à la convention SOCIETE1.) d’un client. Ces deux

messages ne permettraient à aucun moment d'identifier le numéro de téléphone de l'expéditeur, ce qui empêcherait toute vérification de leur provenance réelle et renforcerait leur caractère suspect;

- Le fait que PERSONNE1.) ait reçu deux messages simultanés de deux expéditeurs différents aurait dû l'alerter;

- Ces messages ne feraient en aucun cas mention d'une mise à jour des données informatique relatives à son online Banking SOCIETE1.) via son Token SOCIETE2.), contrairement à ce qu'il affirmerait dans son assignation, ni de sécurisation de son compte bancaire ou d'un piratage en cours, comme il le soutiendrait désormais;

- PERSONNE1.) ne se serait donc pas étonné que la SOCIETE1.), entité indépendante de SOCIETE2.), lui demande de procéder à la mise à jour de son Token SOCIETE2.);

- selon son nouveau récit, il aurait reçu au moins deux messages écrits, ainsi qu'un appel téléphonique frauduleux. Or, PERSONNE1.) ne préciserait pas s'il pensait avoir à faire à son conseiller habituel ou à un tiers inconnu lors de ce prétendu appel et il ne fournirait aucun élément permettant d'identifier cette personne. Il n'indiquerait pas ailleurs aucune diligence qu'il aurait entreprise pour s'assurer de l'identité de son interlocuteur, notamment pour vérifier qu'il s'agissait bien de sa banque. Il n'exposerait pas non plus le prétendu contenu de ce prétendu entretien téléphonique.

  En effet, PERSONNE1.) évoquerait une fraude impliquant des individus usurpant l'identité visuelle et institutionnelle de son établissement bancaire, sans autrement exposer cette affirmation;

- PERSONNE1.) prétendrait avoir confirmé certaines opérations, sans toutefois en préciser leur nature ni fournir la moindre information quant à leur contenu, et transmis des codes d'authentification pour sécuriser ses accès, admettant ainsi avoir communiqué ces informations sensibles à des tiers;

- Il prétendrait également que le site qui se serait ensuite ouvert aurait ressemblé à celui de la SOCIETE1.), sans que PERSONNE1.) ne fournisse davantage de précisions. Il se contenterait d'affirmer que ce site était visuellement crédible. Il ne préciserait pas non plus à quel moment il aurait prétendument cliqué sur le prétendu lien en question, si cela s'est produit en même temps que le prétendu appel téléphonique émanant de sa banque, avant ou après celui-ci, ni quelles opérations il aurait éventuellement réalisées sur ce site.

  En tout état de cause, le prétendu lien ne donnerait aujourd'hui lieu à aucun résultat.

PERSONNE1.) ne se serait donc pas étonné que la SOCIETE1.) lui demande à travers plusieurs communications électroniques de mettre à jour des informations relatives à son Token SOCIETE2.), entité distincte et indépendante de la SOCIETE1.), via un site qui n'aurait rien de commun avec son domaine, ni même avec celui de SOCIETE2.), et qu'elle ne lui en adresse pas la demande à travers la messagerie sécurisée SOCIETE1.).

Il aurait ensuite cliqué sur un lien dont le domaine ne correspondrait ni à celui de la SOCIETE1.), ni à celui de SOCIETE2.), et dont l'extension du pays correspondrait non pas à celle du Grand-Duché de Luxembourg, mais à celle du Liechtenstein;

- La SOCIETE1.) aurait établi moyennant ses pièces que les virements ont été ordonnés suite à 3 authentifications fortes par PERSONNE1.) moyennant ses identifiants personnels SOCIETE2.). PERSONNE1.) aurait nécessairement dû fournir ces éléments, dont le mot de passe à usage unique généré par son Token, à trois différentes reprises. Il le reconnaîtrait d'ailleurs aux termes de ses conclusions.
  Or, la répétition du processus d'authentification à trois reprises moyennant ses identifiants SOCIETE2.) aux seules fins de mettre à jour ses informations, auraient dû alerter PERSONNE1.).

Au vu de ce qui précède, PERSONNE1.) aurait violé ses obligations contractuelles conformément aux articles 25.4 et 27.1 des conditions générales de la SOCIETE1.) dans la mesure où il ne se serait pas assuré de l'authenticité du site sur lequel il aurait inséré ses identifiants SOCIETE2.), malgré plusieurs anomalies apparentes du contexte des messages reçus, de leur contenu et du lien communiqué et il aurait divulgué ses éléments d'identification et de sécurité à une personne tierce, alors que la SOCIETE1.) informerait expressément ses clients qu'elle ne leur demande jamais de se connecter à SOCIETE1.) moyennant un lien.

La violation par PERSONNE1.) de ses obligations contractuelles en ce qui concerne l'instrument de paiement mis à disposition par la SOCIETE1.) serait à qualifier de violation de l'article 83 (1) a) de la loi sur les services de paiement, de sorte qu'il devrait supporter l'intégralité de la perte occasionnée par les virements conformément à l'article 88 (2) de la loi sur les services de paiement.

PERSONNE1.) aurait choisi de suivre aveuglement les instructions qui lui ont prétendument été communiquées, sans aucune remise en question malgré des anomalies apparentes, révélatrices de la prétendue fraude.

Ainsi, PERSONNE1.) ne pourrait raisonnablement prétendre qu'il s'agit en l'espèce d'une fraude d'une particulière complexité. Il s'agirait d'une fraude classique.

Au vu de la négligence grave commise par PERSONNE1.), il y aurait lieu de débouter la demande de celui-ci en ce qu'elle est fondée sur l'article 87 de la loi sur les services de paiement.

Quant au régime de responsabilité de droit commun, la SOCIETE1.) fait valoir que le régime de responsabilité de droit commun ne s'applique pas lorsque le régime de responsabilité mis en place par la loi sur les services de paiement s'applique. Ces deux régimes n'auraient pas vocation à s'appliquer cumulativement à la même situation.

Quant à l'absence d'une violation du devoir de vigilance en l'espèce, PERSONNE1.) soutiendrait également que ce qui aurait dû alerter la SOCIETE1.) résiderait dans le fait que les virements ont été effectués vers des comptes étrangers au bénéfice d'un compte au Portugal, pays avec lequel PERSONNE1.) n'aurait aucune relation. Cette affirmation serait totalement inexacte, puisque les virements auraient en réalité été crédités sur le compte bancaire NUMERO3.) ouvert au nom de PERSONNE3.). Il s'agirait d'un compte luxembourgeois. Les virements ne présentaient aucun risque particulier résultant du facteur géographique.

PERSONNE1.) reprocherait désormais aussi à la SOCIETE1.) un comportement fautif en raison de sa prétendu réaction tardive après le signalement.

La SOCIETE1.) rappelle que ce serait bien elle qui aurait pris l'initiative de contacter PERSONNE1.) le 16 janvier 2023 par voie téléphonique, dans le cadre d'un contrôle du compte de PERSONNE3.). La banque aurait alerté PERSONNE1.) et non l'inverse, alors même que ce dernier ne se serait pas rendu compte de l'existence des virements trois jours après leur exécution.

Le fait que la SOCIETE1.) ait contacté PERSONNE1.) dans le cadre d'un contrôle du compte de PERSONNE3.) témoignerait du fait que les virements avaient d'ores et déjà été crédités sur le compte de celle-ci en date du 16 janvier 2023. Par conséquent, un blocage des comptes en date du 13 janvier 2023 aurait été impossible.

Ceci témoignerait d'une action prompte et efficace, contrairement aux affirmations de PERSONNE1.) et dissiperait tout doute quant au respect par la banque de son devoir de diligence et de vigilance.

Au vu de ce qui précède, la SOCIETE1.) soutient ne pas avoir violé son devoir de vigilance et elle n'aurait commis aucune faute en sa qualité de mandataire de PERSONNE1.).

3. Motifs de la décision

3.1. Quant à la recevabilité de la demande

La demande de PERSONNE1.) n'étant pas énervée quant à sa recevabilité et un moyen d'irrecevabilité à soulever d'office par le Tribunal n'étant pas donné, elle est à déclarer recevable pour avoir été introduite dans les forme et délai de la loi.

3.2. <u>Quant au fond</u>

Conformément à 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. »*

Dans le même sens, l'article 1315 du Code civil dispose que *« 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 ».*

En effet, le demandeur doit démontrer l'existence du fait ou de l'acte juridique sur lequel il fonde sa prétention : *actori incumbit probatio*. Celui qui a fait la preuve des éléments nécessaires à la naissance du droit qu'il invoque ne doit pas, en outre, prouver que ce droit s'est maintenu sans être modifié. Le défendeur se mue en demandeur en tant qu'il invoque une exception : *reus in excipiendo fit actor*. Il lui appartient donc de faire la preuve des faits qu'il invoque à titre d'exception (R. MOUGENOT, Droit des obligations, La preuve, éd. Larcier, 4e éd. 2012, p.108).

En application de l'article 1315 du Code civil, il appartient donc à PERSONNE1.) d'établir la créance de 35.467,92.-euros qu'il invoque à l'encontre de la SOCIETE1.).

PERSONNE1.) soutient qu'il n'a pas donné son consentement aux six transactions qui ont été effectuées en date du 13 janvier 2023 en faveur de PERSONNE3.).

Il se base pour ce faire sur les articles 85 et 87 de la loi du 10 septembre 2009 relative aux services de paiement, à l'activité d'établissement de monnaie électronique et au caractère définitif du règlement dans les systèmes de paiements et les systèmes de règlement des opérations sur titres.

En vertu de l'article 81 de la prédite loi, *« (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.*

(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. (…) »

En vertu de l'article 86 de la prédite loi du 10 septembre 2009, *« (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 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.

(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, 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. »

Il résulte de l'article 30.1. des conditions générales de la SOCIETE1.) que *« (…) dans le cadre des relations entre SOCIETE1.) et le Client, tout ordre ou opération effectués par l'intermédiaire de l'outil électronique moyennant l'utilisation des éléments d'identification du Client tels que prévus par le Login SOCIETE2.) ou par le certificat électronique tiers, ont réputés émaner du Client lui-même. »*

En l'espèce, le Tribunal constate que dans les faits tels que décrits par PERSONNE1.) ne sont pas clairs.

Dans une première phase, dans le cadre de son assignation, il a soutenu qu'il avait, en date du 13 janvier 2024 vers 08.23 heures, procédé à une mise à jour des données informatiques relatives à son online Banking SOCIETE1.) à travers son Token SOCIETE2.) via le lien http://oro.li/SOCIETE1.) qui lui avait été envoyé par message-texte.

Il soutient qu'après avoir cliqué sur le prédit lien, il aurait été orienté vers une application qu'il pensait être l'application de sa banque. Tout aurait été identique au site de la banque, l'accueil, le lay-out, la présentation de la page, les couleurs utilisées. De plus, les messages, textes et indications auraient été sans fautes d'orthographes.

Dans le cadre de ses conclusions ultérieures, PERSONNE1.) soutient avoir reçu un appel téléphonique, ainsi que plusieurs communications émanant d'individus usurpant l'identité visuelle et institutionnelle de la SOCIETE1.) et se faisant passer pour sa banque, ceci notamment par l'apparence du numéro légitime de la SOCIETE1.), des courriels frauduleux reprenant le logo et le style de communication de la banque.

Or, PERSONNE1.) n'indique nullement ce qui lui aurait été dit dans le cadre de son appel téléphonique et il ne verse qu'une capture d'écran, sans expliquer clairement ce qui s'est passé après avoir cliqué sur le lien envoyé.

Aucune pièce n'est versée quant à des courriels frauduleuse reprenant le logo de la SOCIETE1.).

Or, il ressort de l'article 27.1., deuxième alinéa, des conditions générales de la SOCIETE1.) que *« le Client veille à ne pas divulguer ses éléments d'identification et de sécurité (code PIN, mot de passe…), ni à attribuer une autorisation par quelque moyen à une tierce personne sur son outil électronique. SOCIETE1.) ne peut pas être tenue responsable des dommages occasionnés par des opérations exécutées par une tierce personne avec les éléments d'identification ou l'outil du Client. Il est entendu que*

SOCIETE1.) ne demande jamais au Client (par message ou appel téléphonique, courrier électronique ou tout autre moyen) de se connecter à SOCIETE1.) moyennant un lien ou de fournir ses codes d'accès ou autres éléments d'identification et de sécurité. »

Si tant est que PERSONNE1.) n'avait nullement l'intention de virer les montants litigieux à PERSONNE3.), il a tout de même autorisé les six opérations via son dispositif SOCIETE2.).

Compte tenu du fait que PERSONNE1.) a cliqué sur le lien http://oro.li/SOCIETE1.) qui n'est nullement le lien de la banque, mais le lien dont l'extension du pays correspondrait à celle du Liechtenstein, pour par la suite procéder à plusieurs authentifications via SOCIETE2.) sans qu'il ne soit connecté personnellement à SOCIETE1.), il y a lieu de constater que ses agissements sont constitutifs d'une négligence grave.

En présence d'une négligence grave commise par PERSONNE1.), la demande en remboursement formulée sur base de la loi du 10 septembre 2009 est à déclarer non fondée.

PERSONNE1.) reproche encore à la SOCIETE1.) d'avoir manqué à son obligation de vigilance et de diligence.

Dans un arrêt du 2 septembre 2021, la CJUE (aff. C-337/20) a retenu, entre autres, que l'utilisateur d'un service de paiement ne peut engager la responsabilité civile du prestataire de service sur un fondement autre que celui prévu par la directive 2007/64.

Si cet arrêt est intervenu dans le cadre d'une responsabilité recherchée sur base des articles 58, 59 et 60 de la directive 2007/64, transposés aux articles 85, 86 et 87 de la loi sur les services de paiement, il n'en demeure pas moins que dans la motivation du prédit arrêt, la CJUE retient que :
« *41 Or, il convient de relever que l'article 86 de la directive 2007/64, intitulé « Harmonisation totale », dispose que, « [s]ans préjudice d[e plusieurs dispositions de ladite directive qu'il énumère], dans la mesure où la présente directive contient des dispositions harmonisées, les États membres ne peuvent maintenir en vigueur ni introduire des dispositions différentes de celles contenues dans la présente directive ». Aucun des articles 58, 59 et 60 de la même directive ne figure parmi les dispositions pour lesquelles l'article 86 accorde une marge de manœuvre aux États membres pour leur mise en œuvre.*

42 Il s'ensuit que le régime de responsabilité des prestataires de services de paiement prévu à l'article 60, paragraphe 1, de la directive 2007/64 ainsi qu'aux articles 58 et 59 de cette directive a fait l'objet d'une harmonisation totale si bien que les États membres ne peuvent maintenir un régime de responsabilité parallèle au titre du même fait générateur. »

Au vu de ce qui précède, cette jurisprudence est transposable au présent litige.

Il s'ensuit que PERSONNE1.) ne saurait engager la responsabilité de la SOCIETE1.) sur un autre fondement que celui prévu par la loi sur les services de paiement.

La demande de PERSONNE1.) en remboursement de la somme de 35.67,92.-euros est partant à déclarer non fondée.

3.3. Quant aux demandes accessoires

3.3.1. Quant aux frais et honoraires d'avocat

PERSONNE1.) demande encore la condamnation de la SOCIETE1.) à lui payer les frais et honoraires d'avocats déboursés d'un montant de 7.500.-euros.

Il est aujourd'hui de principe que les honoraires que le justiciable doit exposer pour obtenir gain de cause en justice constituent un préjudice réparable qui trouve son origine dans la faute de la partie qui succombe (Cour de cassation, 9 février 2012, arrêt n° 5/12, JTL 2012, n° 20, page 54 ; CA, 9ème chambre, 20 novembre 2014, n° 39.462 du rôle). Les frais et honoraires d'avocat peuvent ainsi donner lieu à indemnisation sur base de la responsabilité civile de droit commun en dehors de l'indemnité de procédure.

PERSONNE1.) doit établir les conditions légales pour se voir allouer les honoraires d'avocats, à savoir la preuve d'une faute, d'un dommage et d'un lien causal.

Il y a lieu de rappeler que l'exercice de l'action en justice est un droit fondamental tout comme le droit corollaire pour une partie de se défendre dans le cadre d'une telle action, de sorte que le fait de succomber à la demande adverse ne constitue pas automatiquement un comportement fautif pour la partie défenderesse.

L'exercice de l'action en justice n'est susceptible de donner lieu à réparation, sur le fondement des articles 1382 ou 1383 du Code civil, que lorsqu'il dégénère en abus, lequel suppose, dans le chef de son auteur, une intention malveillante, une erreur grossière équipollente au dol ou une légèreté blâmable.

La faute qui est reprochée doit par conséquent être une faute distincte de celle qui lui a été reprochée et qui a mené à l'introduction de l'action en justice.

En l'espèce, PERSONNE1.) a succombé dans ses demandes.

La demande de celui-ci en remboursement des frais et honoraires d'avocats est partant à déclarer non fondée.

3.3.2. Quant à l'indemnité de procédure

PERSONNE1.) demande à ce que la SOCIETE1.) soit condamnée à lui payer le montant de 3.000.- euros sur la base de l'article 240 du Nouveau Code de procédure.

La SOCIETE1.) demande à ce que PERSONNE1.) soit condamné à lui payer le montant de 5.000.-euros sur base de l'article 240 du Nouveau Code de procédure civile.

L'application de l'article 240 du Nouveau Code de procédure civile relève du pouvoir discrétionnaire du juge (Cass., 2 juillet 2015, arrêt n° 60/15, JTL 2015, n° 42, page 166).

Au vu de l'issue du litige, PERSONNE1.) est à débouter de sa demande en allocation d'une indemnité de procédure.

N'ayant pas justifié en quoi il serait inéquitable de laisser à leur charge l'intégralité des frais non compris dans les dépens, la demande de la SOCIETE1.) en paiement d'une indemnité de procédure est à déclarer non fondée.

3.3.3. Quant aux frais et dépens de l'instance

En application des articles 238 et 242 du Nouveau Code de procédure civile, toute partie qui succombera sera condamnée aux dépens, à moins que le juge, par décision spéciale et motivée, n'en mette la totalité ou une fraction à la charge de l'autre partie et les avocats à la Cour pourront, dans les instances où leur ministère est obligatoire, demander la distraction des dépens à leur profit.

Au vu de l'issue du litige, il y a lieu de condamner PERSONNE1.) aux frais et dépens de l'instance, avec distraction au profit de Maître Géraldine MERSCH, qui la demande, affirmant en avoir fait l'avance.

PAR CES MOTIFS

le tribunal d'arrondissement de et à Luxembourg, huitième chambre, siégeant en matière civile, statuant contradictoirement ;

reçoit la demande en la forme ;

la dit non fondée ;

déboute PERSONNE1.) de sa demande en condamnation de la SOCIETE1.) au montant de 7.500.-euros à titre de frais et honoraires d'avocats sur base des articles 1382 et 1383 du Code civile ;

dit non fondées les demandes respectives de PERSONNE1.), d'une part, et de la SOCIETE1.), d'autre part, en allocation d'une indemnité de procédure sur base de l'article 240 du Nouveau Code de procédure civile ;

condamne PERSONNE1.) aux frais et dépens de l'instance avec distraction au profit de Maître Géraldine MERSCH, avocat, qui la demande, affirmant en avoir fait l'avance.