Conditions d'accès et d'utilisation des Services E-Banking (banque en ligne)

Le présent document complète les Conditions Générales de la Banque de Luxembourg (ci-après la « Banque ») qui ont vocation à s'appliquer à toutes les relations du Client avec la Banque et notamment à la détermination du droit applicable et à la désignation de la juridiction compétente.

1. Objet

Les présentes conditions régissent l'accès et l'utilisation par le Client des services de banque en ligne via le site E-Banking et/ou via l'application BL-Mobile Banking (ci-après les « Services E-Banking ») de la Banque, ainsi que des modalités de preuve des échanges et des transactions réalisés sur un ou plusieurs comptes auprès de la Banque sur lesquels il a un pouvoir de signature soit en tant que titulaire soit en tant que représentant ou mandataire (ci-après « les Comptes Consultables »).

Ces Conditions d'accès et d'utilisation des Services E-Banking ne créent aucune nouvelle obligation d'information ou de conseil, ni aucun nouveau mandat à la charge de la Banque.

Les Services E-Banking de la Banque offrent notamment les fonctionnalités suivantes :

– Présentation de la Banque, de ses produits et services,

– Informations sur les marchés,

– Informations sur les opérations / événements sur titres et possibilité de donner des instructions y relatives,

– Recherche et analyse financière,

– Consultation des Comptes Consultables,

– Possibilité d'effectuer certaines transactions,

– Communications par voie électronique,

– Consultation et génération de documents,

– Signature électronique de documents et d'instructions,

– Détermination / changement de certaines données personnelles ainsi que, pour certains clients éligibles, la possibilité de télécharger des documents dans le cadre de la mise à jour du dossier client,

– Agrégation de comptes détenus auprès d'autres prestataires de services de paiement,

– La mise à disposition, via un sous-traitant, d'une plateforme permettant de centraliser et gérer des données et documents signalétiques, voire, si le Client en décide ainsi, la possibilité de mutualiser ces informations et documents avec les banques auprès desquelles le Client entretient aussi des relations bancaires et qui utilisent la même plateforme.

Par cet accès aux Services E-Banking, le Client reconnaît et accepte que le Mandataire pourra visualiser, le cas échéant, les cartes de crédit liées aux Comptes Consultables, pourra demander leur blocage, modifier le montant de leur limite d'utilisation et procéder à l'activation du service 3D Secure conformément aux Conditions générales des cartes de paiement.

Certaines des fonctionnalités mentionnées ci-dessus peuvent être exclusives à certains clients éligibles ou être exclusives ou se présenter différemment sur l'espace E-Banking du site internet de la Banque ou dans l'application BL-Mobile Banking.

La Banque se réserve le droit de modifier à tout moment ces fonctionnalités.

2. Frais

L'accès aux Services E-Banking est facturé selon les tarifs en vigueur auprès de la Banque, que le Client déclare connaître et accepter. Les autres frais tels que l'abonnement Internet (Internet Service Provider), les frais d'itinérance (roaming) et de services de données (data) ou autres, sont à la charge du Client.

Les Tarifs et Conditions de la Banque relatifs aux opérations de virement, aux ordres de bourse, aux taux d'intérêt et aux taux de change sont applicables.

3. Sécurité des Services E-Banking

3.1. Modes d'accès

Pour accéder aux Services E-Banking, le Client veillera à disposer d'une connexion au réseau Internet auprès du fournisseur d'accès de son choix. La Banque n'assume aucune responsabilité en relation avec la connexion du Client au réseau Internet, qui se fait aux risques et périls exclusifs du Client.

L'accès aux Services E-Banking s'effectue via l'application BL-Mobile Banking ou via l'adresse du site E-Banking communiquée au Client avec ses identifiants ou toute autre adresse que la Banque communiquera au Client par tout moyen qu'elle jugera approprié et notamment par voie électronique.

Si le moyen d'accès aux Services E-Banking est un Signing Server LuxTrust (LuxTrust Scan ou LuxTrust Mobile App), le Client recevra sous enveloppe ou par SMS de la part de LuxTrust les identifiants correspondant à son choix afin de lui permettre de se connecter aux Services E-Banking, de s'identifier et de signer ses instructions. Dès mémorisation des identifiants, le SMS ou l'imprimé doivent être détruits. Si le moyen d'accès aux Services E-Banking est un autre moyen d'authentification reconnu par LuxTrust alors le Client recevra les modalités et les conditions d'utilisation par le fournisseur de sa solution d'authentification.

Tout support utilisé pour l'authentification lui sera, le cas échéant, remis ou envoyé dans une enveloppe séparée.

Le Client autorise expressément la Banque et LuxTrust à remettre à ses mandataires, présents ou futurs, qui ont un pouvoir de signature ou un droit de regard sur les Comptes Consultables via la banque en ligne, des identifiants et moyens d'authentification donnant accès aux Services E-Banking, lorsque ces derniers le demandent.

3.2. Devoirs de diligence du Client

Afin de prévenir toute utilisation frauduleuse, le Client s'oblige à protéger tous ses identifiants et s'engage à prendre toute mesure de sécurité afin de garder le contrôle exclusif sur son mode d'authentification d'accès (support d'authentification et identifiant reçus par LuxTrust ou par un autre fournisseur de sa solution d'authentification reconnue, mot de passe, One Time Password) qu'il est le seul à connaître et à détenir. Il est de sa responsabilité exclusive de conserver ces codes personnels strictement confidentiels. Ils ne doivent être ni notés, ni communiqués ou transmis à une tierce personne, ni enregistrés sur la mémoire d'un ou de plusieurs appareils.

Le Client déclare prendre note du fait que la Banque ne sollicitera jamais le Client par téléphone, courrier électronique, SMS ou tout autre moyen de communication pour obtenir des informations confidentielles (son identifiant, mot de passe, son One Time Password) ou pour l'inviter à se connecter aux Services E-Banking de la Banque via un lien repris dans le courrier électronique ou SMS.

Le Client peut donc considérer comme suspect tout courrier électronique ou SMS non sollicité qui prétendrait provenir de la Banque et qui lui demanderait de communiquer ses coordonnées personnelles et/ou mot de passe. Par ailleurs, la Banque conseille à son Client de saisir lui-même l'adresse https://www.banquedeluxembourg.com, de vérifier qu'il n'y a pas de faute d'orthographe et de ne pas suivre un lien contenu dans un courrier électronique ou SMS.

Le Client s'engage par ailleurs à prendre connaissance des risques décrits dans l'annexe « Avertissement sur les risques inhérents aux virements effectués via les Services E-Banking

(banque en ligne) » et à respecter les recommandations et consignes de sécurité contenues dans les « Infos sécurité » du site E-Banking et/ou de l'Application BL-Mobile Banking ainsi que dans l'annexe « Que peut-on faire pour réduire les risques ? Revue des bonnes pratiques de sécurité sur Internet ».

Le non-respect de ces consignes de sécurité est à considérer comme une négligence grave et mettra le Client dans l'obligation de supporter l'entière perte pouvant, le cas échéant, résulter d'un accès frauduleux aux Services E-Banking.

3.3. Blocage de l'accès aux Services E-Banking

3.3.1. À la demande du Client

Dès l'instant où le Client sait ou soupçonne qu'un tiers puisse accéder aux Services E-Banking suite à la perte, au vol, au détournement ou à l'utilisation non autorisée de l'un de ses éléments d'identification, il en informe immédiatement la Banque et LuxTrust ou tout autre fournisseur de sa solution d'authentification, afin que ceux-ci puissent bloquer un tel accès, du lundi au vendredi de 08.00 à 18.00 heure :

assistance LuxTrust : (+352) 24 550 550

assistance BL-Support : (+352) 26 20 26 30

En cas d'accès aux Services E-Banking par un autre moyen d'authentification, le Client s'adressera à l'assistance du fournisseur de cette autre solution d'authentification.

En dehors des jours ouvrés, le Client procédera au blocage de son dispositif LuxTrust, qui est possible à toute heure, 7 jours sur 7, depuis le site de LuxTrust (https://www.luxtrust.lu/fr/management).

En cas d'accès aux Services E-Banking par un autre moyen d'authentification, le Client consultera le site web du fournisseur de cette autre solution d'authentification.

3.3.2. À l'initiative de la Banque

Lorsque les règles de détection de la Banque indiquent un soupçon de fraude, une fraude avérée ou des menaces pour la sécurité de l'accès aux Services E-Banking du Client, en particulier en cas de soupçon de fraude sur virement, la Banque contactera le Client par tout moyen qu'elle jugera utile et, le cas échéant, l'informera que son accès aux Services E-Banking a été restreint ou bloqué afin de limiter le risque d'utilisation non autorisée ou frauduleuse, sans que cette procédure sécuritaire entraîne une quelconque obligation ou responsabilité dans le chef de la Banque.

La Banque se réserve le droit de restreindre, de bloquer ou de retirer définitivement l'accès aux Services E-Banking du Client lorsque celui-ci ne respecte pas ses obligations ou les recommandations de la Banque ou si celle-ci estime prudent d'interdire l'accès au Client pour toute autre raison objectivement motivée ayant trait notamment, mais non limitativement :

- **à la sécurité de l'accès aux Services E-Banking ;**
- **en cas de constatation, simple présomption ou risque d'accès illicite, non autorisé, abusif ou frauduleux ;**
- **en vue de préserver les intérêts du Client ou de la Banque ;**
- **lorsque les comptes sont clôturés ou bloqués ou s'il s'avère que le Client ne respecte pas ses obligations légales, réglementaires ou contractuelles en rapport avec les services proposés ;**
- **sur demande d'une autorité judiciaire ;**
- **en cas de décès d'un des titulaires de compte ;**
- **s'il s'agit d'un accès aux Services E-Banking doté d'un découvert accordé par la Banque, au risque sensiblement accru que le Client soit dans l'incapacité de s'acquitter de son obligation de paiement d'une ligne de crédit.**

Dans ces cas, la Banque informe le Client du blocage et des raisons du blocage, au plus tard immédiatement après le blocage, à moins que le fait de fournir cette information ne soit pas acceptable pour des raisons de sécurité ou interdit en vertu de la législation applicable. La Banque débloque l'accès ou remplace celui-ci par un nouvel accès dès lors que les raisons justifiant le blocage n'existent plus.

3.4. Accès et sécurité

La connexion aux Services E-Banking est protégée par une solution de chiffrement et d'identification du Client.

Le Client reconnaît avoir reçu de la part de la Banque toutes les précisions utiles sur ce dispositif de sécurité, son efficacité et ses limites. Il l'accepte comme satisfaisant et décharge formellement la Banque de toute responsabilité concernant les conséquences d'une violation du dispositif de sécurité par un tiers non autorisé. Il autorise également la Banque à modifier le fonctionnement pratique et technique des Services E-Banking et, en particulier, le dispositif de sécurité permettant de s'y connecter, notamment pour tenir compte d'une évolution des technologies. Le Client en sera dûment prévenu par les moyens que la Banque jugera adéquats.

Le Client s'engage à respecter strictement les procédures d'accès aux Services E-Banking telles qu'elles lui ont été indiquées par la Banque ainsi que toutes les consignes d'utilisation affichées via les Services E-Banking ou communiquées au Client par tout autre moyen. Il vérifiera à chaque connexion le caractère sécurisé de la communication. En cas de non-respect de cette procédure ou des consignes d'utilisation, comme dans l'hypothèse d'une tentative de connexion aux Services E-Banking au moyen d'un identifiant incorrect, la Banque se réserve le droit de refuser au Client tout nouvel accès aux Services E-Banking.

D'un commun accord entre les parties, tout accès aux Services E-Banking effectué à l'aide de l'un des identifiants du Client est réputé l'être par le Client, le journal des connexions tenu par la Banque faisant foi de celles-ci.

De la même manière, tout accès aux Services E-Banking par un mandataire ou un représentant du Client effectué à l'aide de l'un des identifiants de ce mandataire ou représentant est réputé être effectué par ce mandataire ou représentant au nom et pour le compte du Client; ce dernier reste entièrement responsable des actes et omissions, même involontaires, de ses mandataires ou représentants dans le cadre de leur utilisation des Services E-Banking, jusqu'à révocation de leur accès à l'initiative du Client, de ses mandataires ou représentants, ou de la Banque.

Sauf en cas de faute grave ou de négligence de sa part, la Banque n'encourt aucune responsabilité et ne saurait en particulier se voir reprocher une violation de son obligation au secret au cas où un tiers aurait pu accéder aux Comptes Consultables du Client ou obtenir, grâce au site E-Banking et/ou à l'application BL-Mobile Banking de la Banque ou au réseau Internet, des renseignements sur sa relation avec la Banque.

4. Informations accessibles via les Services E-Banking

Le Client peut consulter via les Services E-Banking diverses informations d'ordre financier ou économique, émanant de la Banque aussi bien que de tiers et portant notamment sur les marchés financiers et les fonds d'investissement.

La Banque indiquera, dans la mesure du possible, la date de parution ou de création des informations publiées via les Services E-Banking et tiendra ces informations à jour aussi rapidement que celles distribuées sur support papier.

Dans le cadre de ses investissements en titres, le Client peut consulter via les Services E-Banking les opérations sur titres (ci-après les « OST »), et communiquer par voie électronique les ordres y liés conformément à l'article 6.2 des présentes conditions.

L'ensemble des informations publiées via les Services E-Banking l'est à titre purement indicatif et ne saurait être assimilé à un quelconque conseil de la part de la Banque. Le Client s'oblige à utiliser ces informations avec discernement et esprit critique.

Il décharge expressément la Banque de toute responsabilité quant au contenu, à la fiabilité, à l'actualité, à l'intégrité ou à l'exactitude des informations provenant de tiers et signalées comme telles. Il déclare être conscient que les OST se basent sur des informations reçues de sources externes qui n'ont pas été vérifiées par la Banque.

Le Client renonce expressément à tout conseil en ligne de la part de la Banque à propos des informations publiées via les Services E-Banking et s'engage à recueillir tout conseil relatif à ses investissements et à la gestion de son portefeuille directement auprès du conseiller de son choix.

Le Client s'engage à respecter la propriété des informations accessibles via les Services E-Banking et s'interdit de les communiquer à des tiers, de les publier ou de les diffuser par quelque moyen et à quelque titre que ce soit ainsi que de reproduire tout ou partie des Services E-Banking. Sauf opposition écrite, il autorise la Banque à lui adresser toute communication, y compris de nature commerciale, par le biais des Services E-Banking ou par courrier électronique.

5. Consultation des Comptes Consultables

Le Client peut consulter via les Services E-Banking la situation des Comptes Consultables et, le cas échéant, les opérations d'achat et de vente en cours d'exécution sur ces mêmes comptes. Il autorise la Banque à lui communiquer par le réseau Internet toute information sur les Comptes Consultables et les opérations faites sur ces comptes et ce nonobstant un éventuel accord avec la Banque aux termes duquel la correspondance qui lui est destinée doit être tenue à sa disposition dans les locaux de la Banque.

Le Client qui a opté pour une consultation des Comptes Consultables dont il est titulaire ou représentant exclusivement via les Services E-Banking, s'engage à les consulter au moins une fois par trimestre. A défaut de consultation des Comptes Consultables pendant une période continue de six mois, la Banque désactivera l'accès aux Services E-Banking et lui fera suivre à ses frais les extraits de compte, les relevés de la situation et la correspondance relative aux Comptes Consultables à l'adresse définie dans la demande d'ouverture de compte ou communiquée ultérieurement par le Client.

La Banque se réserve le droit de refuser au Client l'accès aux Services E-Banking sur un ou plusieurs Comptes Consultables si elle estime de manière discrétionnaire avoir une raison valable de le faire.

6. Ordres électroniques du Client

Les Services E-Banking permettent au Client de transmettre à la Banque des ordres de virement, des ordres d'achat ou de vente d'instruments financiers ainsi que tout ordre en rapport avec les OST liées à ses investissements (ci-après « les Ordres Electroniques ») qui seront exécutés dans les mêmes conditions que ses autres ordres, et d'apposer sa signature électronique sur des documents lui transmis par la Banque; cette signature électronique aura même valeur qu'une signature manuscrite.

Pour chaque Ordre Electronique adressé à la Banque, le Client s'engage à donner les précisions nécessaires à la bonne exécution de l'ordre. La Banque affichera à l'écran le détail des informations saisies par le Client.

A l'exception d'une autorisation accordée au Client en vertu d'un découvert accordé par la Banque au Client, le Client ne peut opérer que sur base créditrice et dans les limites d'une couverture suffisante du compte. Le Client s'engage à approvisionner le compte courant afin que le crédit figurant sur ce compte courant soit suffisant pour faire face aux Ordres Electroniques dans les limites d'utilisation définies. Le Client reconnaît qu'à défaut, le compte produira des intérêts débiteurs tels que prévus à l'article 15 des Conditions Générales de la Banque. La Banque se réserve le droit de refuser tout Ordre Electronique si le compte n'est pas suffisamment approvisionné.

Le Client répond de tous les ordres transmis grâce à ses identifiants jusqu'à ce qu'il ait prévenu la Banque de ne plus s'y fier selon la procédure décrite à l'article 3.3. ci-dessus et que celle-ci ait été en mesure de rejeter de tels ordres.

Le Client est responsable de tous les Ordres Electroniques transmis via les Services E-Banking par lui-même, son mandataire ou son représentant, et cela malgré le fait que la procuration en faveur d'un mandataire ou d'un représentant ait été révoquée.

Les parties reconnaissent aux Ordres Electroniques transmis, ainsi qu'aux documents signés électroniquement au travers des Services E-Banking de la Banque, la valeur probante d'un acte sous seing privé conformément aux articles 1322 et suivants du code civil et leur opposabilité en tant que tels au Client et à la Banque quel qu'en soit le montant ou la portée.

6.1. Ordres sur instruments financiers

Les ordres d'achat ou de vente d'instruments financiers sont présumés être donnés en exécution et/ou en réception et transmission d'ordres en exécution simple visés à l'article 12 des Conditions Générales de la Banque.

6.2. Ordres en lien avec des opérations sur titres

Si le Client est amené à donner un ordre suite à la consultation d'une OST via les Services E-Banking (l' « Ordre »), il déclare être conscient que les Services E-Banking constituent le seul canal de communication.

Le Client déclare accepter que la Banque ne s'assure pas de la conformité de l'Ordre aux lois et règlements applicables et/ou à toute autre restriction en cause. Il déclare ainsi accepter toute conséquence résultant de l'Ordre.

Le Client déclare accepter que les Ordres communiqués via les Services E-Banking grâce à ses codes personnels sont transmis à ses risques et périls et décharge la Banque de toute responsabilité résultant d'un comportement négligent ou fautif de sa part ainsi que du non-respect des règles de conduite reprises dans les présentes conditions et ses annexes.

Plus particulièrement, le Client décharge la Banque de toute responsabilité résultant d'un retard dans la communication de l'OST et/ou dans la transmission de l'Ordre.

6.3. Ordres de virement

6.3.1. Déclaration d'acceptation des risques

Le Client déclare être conscient de tous les risques inhérents à l'exécution de virements via les Services E-Banking tels qu'exposés dans l'annexe « Avertissement sur les risques inhérents aux virements effectués via les Services E-Banking (banque en ligne) ».

Le Client déclare être conscient que les risques de pertes inhérents aux virements effectués via les Services E-Banking sont accrus en cas d'augmentation de la limite de ses virements.

Le Client déclare accepter que tous les virements effectués sur les Services E-Banking grâce à ses codes d'accès personnels soient exécutés à ses risques et périls et décharge la Banque de toute

responsabilité résultant d'un comportement négligent ou fautif de sa part ainsi que du non-respect des règles de conduite reprises dans le présent document et ses annexes.

6.3.2. Consentement et révocation des ordres de virement, délai d'exécution

Un ordre de virement est réputé autorisé si le Client a donné son consentement à son exécution grâce au mode d'authentification et de validation exigé par les Services E-Banking. En l'absence d'un tel consentement, l'ordre de virement est réputé non autorisé.

Les dispositions concernant le moment de la réception de l'ordre de virement et la révocation de l'ordre de virement ainsi que le délai d'exécution maximal, mentionnées à l'article 9 des Conditions Générales de la Banque, s'appliquent pleinement.

6.3.3. Responsabilité du Client en cas d'opérations de virement non autorisées

Le Client consommateur peut être tenu de supporter, jusqu'à concurrence de 50 EUR et jusqu'à la notification de toute perte, vol ou contrefaçon des identifiants aux Services E-Banking, les pertes liées à toute opération de virement non autorisée consécutive à l'utilisation ou au détournement de ses identifiants aux Services E-Banking. Cette clause ne s'applique pas si la perte, le vol ou le détournement des accès ne pouvait être détecté par le Client avant le paiement, sauf si le Client a agi frauduleusement, ou si la perte est due à des actes ou à une carence d'un salarié, d'un agent ou d'une succursale de la Banque, LuxTrust ou d'un autre fournisseur de la solution d'authentification.

Le plafond maximal de 50 EUR n'est pas d'application pour le Client non-consommateur.

Le Client, qu'il soit consommateur ou non-consommateur, supporte toutes les pertes occasionnées par des opérations de virement non autorisées si ces pertes résultent soit d'un agissement frauduleux de sa part, soit du fait qu'il n'a pas satisfait, intentionnellement ou à la suite d'une négligence grave, à une ou plusieurs des obligations mentionnées dans l'article 3 des présentes conditions. Dans ce cas le montant maximal indiqué ci-dessus ne s'applique pas. Sont notamment considérées comme négligences graves, le fait pour le Client de noter ses dispositifs de sécurité personnalisés, comme son identifiant personnel, ou tout autre code, sous une forme aisément reconnaissable, le fait de les avoir communiqués à une tierce personne, ou le fait de les avoir enregistrés sur la mémoire d'un ou de plusieurs appareils de manière non sécurisée, ainsi que le fait de ne pas avoir notifié au service central de mise en opposition la perte ou le vol, dès qu'il en a eu connaissance. Pour l'appréciation de la négligence, il sera tenu compte de l'ensemble des circonstances de fait.

Dans le cas où la Banque aurait remboursé au Client le montant correspondant à une opération non autorisée et qu'elle a ensuite de bonnes raisons de soupçonner que le Client a agi frauduleusement ou n'a pas satisfait, intentionnellement ou à la suite d'une négligence grave, à une ou plusieurs des obligations mentionnées ci-dessus, la Banque se réserve le droit de prélever ce montant sur le compte du Client et d'en informer la Commission de Surveillance du Secteur Financier (CSSF), établie à L-1150 Luxembourg, 283 route d'Arlon.

6.3.4. Droit au remboursement, notification et correction d'opérations de virement non autorisées ou mal exécutées

Les conditions relatives au droit au remboursement, à la notification et la correction d'opérations de paiement non autorisées ou mal exécutées sont régies par les dispositions correspondantes à l'article 9 des Conditions Générales de la Banque.

6.4. Inscription en compte des Ordres Electroniques

Les Ordres Electroniques sont exécutés par inscription en compte et sont assimilés aux opérations décrites aux articles 9 et 12 des Conditions Générales de la Banque. Toute inscription en compte d'une transaction non autorisée, toute erreur ou autre irrégularité dans la gestion du compte doivent être immédiatement signalées à la Banque.

La Banque s'engage à conserver sur un support durable, pendant une durée de 10 ans, un exemplaire de tous les Ordres Electroniques transmis du Client, en prenant toutes les mesures de sécurité garantissant l'inaltérabilité de ces enregistrements. Le Client accepte expressément que les enregistrements par la Banque de ses Ordres Electroniques transmis fassent foi de leur existence, de leur contenu et de leur date et heure précises et puissent être produits à cette fin en justice. La Banque fournira sur demande du Client une copie de tous ces enregistrements.

7. Réclamations du Client

Les conditions relatives aux réclamations, y compris les voies de recours extrajudiciaires ouvertes au Client, sont reprises à l'article 7 des Conditions Générales de la Banque.

8. Service d'agrégation des comptes

Le service d'agrégation des comptes correspond au service d'information sur les comptes selon les dispositions de la PSD2[1]. Il consiste à fournir, en ligne, des informations consolidées concernant le(s) compte(s) de paiement détenu(s) et désigné(s) par le Client auprès d'un ou de plusieurs prestataires de services de paiement désignés par le Client, c'est-à-dire, entre autres, le solde de ce(s) compte(s) et les opérations de paiement exécutées durant les 90 derniers jours par l'intermédiaire de ce(s) compte(s) de paiement désigné(s).

La Banque ne peut transmettre au Client que les informations fournies par le ou les prestataires de services de paiement désignés par le Client ; elle ne pourra être tenue responsable d'un quelconque défaut d'information dans le chef de ce(s) prestataire(s) de services de paiement.

Le service d'agrégation des comptes n'est pas subordonné à l'existence de relations contractuelles entre la Banque et les autres prestataires de services de paiement. Il est fourni sur base du consentement explicite du Client et de son authentification adéquate auprès des autres prestataires de service de paiement, à condition que les comptes désignés soient accessibles en ligne et que le Client soit titulaire des Comptes Consultables auprès de la Banque. Le consentement du Client sera exigé lorsque celui-ci accède pour la première fois au service d'agrégation des comptes ; il expirera et devra être renouvelé 90 jours plus tard.

Dans le cadre du service d'agrégation des comptes, le Client autorise expressément la Banque à utiliser ses données de sécurité personnalisées afin de permettre au Client de s'identifier de manière sécurisée auprès du ou des prestataires de services de paiement désignés par le Client. La Banque veille à ce que les données de sécurité personnalisées du Client ne soient pas accessibles à d'autres parties que le Client et l'émetteur desdites données et utilise des canaux sûrs et efficaces pour la transmission de ces données.

La Banque accède uniquement aux informations provenant des comptes désignés par le Client et des opérations de paiement associées. La Banque n'utilise, ne consulte ou ne stocke des données à des fins autres que le service d'agrégation des comptes, conformément aux règles relatives à la protection des données.

1 Directive (UE) 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur, modifiant les directives 2002/65/CE, 2009/110/CE et 2013/36/UE et le règlement (UE) n o 1093/2010, et abrogeant la directive 2007/64/CE

9. Traitement et protection des données personnelles

L'accès aux Services E-Banking implique le traitement par la Banque des données à caractère personnel du Client, à des fins d'exécution du présent contrat et de gestion globale de la relation client et des services liés.

Les informations recueillies à l'aide de la Demande d'accès aux Services E-Banking peuvent ainsi être mises sur tout support et sont enregistrées par la Banque, dans un fichier informatisé et traitées aux fins d'identification et de gestion des accès aux Services E-Banking, de la gestion des comptes et des opérations, ainsi que du contrôle de leur régularité.

Afin de répondre à ses obligations réglementaires, notamment au regard de la législation en matière de lutte contre le blanchiment d'argent et contre le financement du terrorisme, la Banque peut être amenée à vérifier l'authenticité des données fournies par le Client et à transférer ces données aux autorités publiques et aux juridictions compétentes.

La Banque pourra conserver les données personnelles pour une durée n'excédant pas celle nécessaire au regard des finalités poursuivies par la Banque et suivant les modalités reprises dans les Conditions Générales de la Banque.

En vue de l'exécution du présent contrat et de la fourniture des Services E-Banking, la Banque transfère les données personnelles du Client à la société LuxTrust et/ou à tout autre fournisseur de la solution d'authentification choisie par le Client et reconnue par LuxTrust, ainsi que, pour les besoins du service d'agrégation des comptes, à la société LuxHub, gestionnaire de l'interface (API), qui procéderont également dans ces contextes au traitement des données, auquel le Client donne son accord explicite. Le Client bénéficie du droit de demander l'accès, la rectification, l'effacement et la portabilité de ses données à caractère personnel, celui de s'opposer à leur traitement ou encore d'en demander une limitation.

Le Client peut consulter et/ou modifier certaines données personnelles via les Services E-Banking. Le Client demande à ce que tout changement ainsi notifié à la Banque soit pris en compte par elle dans les mêmes conditions que toute autre notification de changement.

Le Client s'engage à fournir des données correctes et exactes à la Banque, à informer la Banque dans les meilleurs délais de tout changement de ces données et à communiquer à la Banque sur simple demande tout document ou renseignement complémentaire que celle-ci jugerait utile dans le cadre du maintien des relations bancaires ou qui serait requis par des dispositions légales ou réglementaires.

Afin d'améliorer l'expérience du Client dans le cadre de l'obligation de vigilance de la Banque à l'égard de sa clientèle (KYC), la Banque peut être amenée à recourir aux services d'un sous-traitant pour mettre à disposition des clients éligibles une plateforme permettant la centralisation et la gestion électronique de leurs données et documents signalétiques (le «Service de gestion des données »). En vue de l'exécution de ce service, la Banque transfère des données personnelles du Client à son sous-traitant. Ce Service de gestion des données permet aux clients éligibles de centraliser et gérer leurs données et documents signalétiques, ces derniers étant susceptibles de recevoir des notifications du sous-traitant pour les informer lorsque des données ou documents ne sont plus à jour.

Le Client éligible à ce Service de gestion des données en est informé via son accès aux Services E-Banking et s'engage à accepter les conditions d'utilisation de ce Service de gestion des données du sous-traitant en activant ce dernier. Le défaut et/ou le refus du Client d'accepter ces dernières peut être considéré par la Banque comme un obstacle à la fourniture des Services E-Banking, voire même au maintien des relations d'affaires avec la Banque.

Le Client éligible à ce Service de gestion des données a également la possibilité d'opter pour le partage de certaines données et certains documents signalétiques avec ses autres banques avec lesquelles le Client a également une relation bancaire et qui utilisent la même plateforme du sous-traitant. Pour bénéficier de cette mutualisation de données, le Client devra confirmer son souhait de le faire via les Services E-Banking et/ou via les services équivalents des autres banques auprès desquelles le Client entretient des relations bancaires et qui utilisent la même plateforme. Le Client ayant opté pour ce service de mutualisation de données déclare avoir pris connaissance et approuver les conditions générales d'utilisation de ce service de mutualisation et toutes autres conditions le liant et/ou liant la Banque au sous-traitant dans le cadre de ce service.

Les présentes dispositions concernant le traitement et la protection des données personnelles du Client viennent en complément de l'article 22 des Conditions Générales de la Banque ainsi que de la Data Privacy Policy que le Client déclare approuver et accepter.

10. Accessibilité des Services E-Banking

La Banque se réserve le droit de suspendre temporairement l'accès aux Services E-Banking, notamment pour des raisons d'ordre technique.

Lorsque la Banque est en mesure de prévoir l'inaccessibilité temporaire aux Services E-Banking, elle fera de son mieux pour en informer préalablement le Client par tous moyens appropriés, y compris par un message transmis par les Services E-Banking.

Le Client décharge la Banque de toutes les conséquences pouvant résulter d'une inaccessibilité temporaire des Services E-Banking, pour quelque cause que ce soit, ainsi que de toutes les conséquences pouvant résulter d'un ralentissement, d'une panne ou d'un dysfonctionnement des Services E-Banking, de l'infrastructure informatique de la Banque, d'une déconnexion aux Services E-Banking ou de tout autre incident technique même imputable à la Banque.

11. Confidentialité des messages

Les parties reconnaissent aux messages échangés via les Services E-Banking le caractère d'une correspondance privée.

12. Localisation des échanges

Les communications établies entre la Banque et le Client, ainsi que toutes les opérations initiées ou réalisées au travers des Services E-Banking sont réputées être effectuées directement à la Banque, à la date et l'heure indiquées sur le serveur de la Banque, le journal des connexions tenu par la Banque faisant foi de celles-ci.

13. Destruction des identifiants et certificats

Dans l'hypothèse où le Client n'a plus d'accès à ses Comptes Consultables via les Services E-Banking, il s'engage à détruire tous les moyens d'authentification lui ayant été remis par la Banque.

14. Responsabilité

Dans le cadre de la mise à disposition des Services E-Banking, la Banque n'assume que des obligations de moyens à l'égard du Client. Conformément à l'article 21 des Conditions Générales de la Banque, la responsabilité de la Banque ne peut être engagée que pour faute grave.

La Banque ne peut encourir aucune responsabilité en cas de force majeure ou lorsqu'elle est liée par d'autres obligations légales en vigueur.

Le Client qui accède aux Services E-Banking à partir de l'étranger s'engage à se conformer au respect des prescriptions légales et réglementaires en vigueur dans le pays à partir duquel cet accès a lieu.

La Banque ne peut encourir aucune responsabilité en cas de défaillance des solutions d'authentification fournies par le fournisseur de la solution d'authentification choisie par le Client.

15. Modifications des Conditions d'accès et d'utilisation des Services E-Banking

La Banque peut modifier à tout moment les présentes Conditions d'accès et d'utilisation des Services E-Banking par une notification écrite au Client, par tous moyens y compris par un message transmis ou affiché via les Services E-Banking, selon les modalités de l'article 23 des Conditions Générales.

Toute utilisation des Services E-Banking après notification de la modification entraîne l'acceptation d'office de celle-ci par le Client.

La nullité ou l'inapplicabilité de l'une des clauses des présentes Conditions d'accès et d'utilisation des Services E-Banking n'affectera pas la validité des autres clauses qui demeurent applicables en l'absence des dispositions annulées.

16. Durée et résiliation du contrat

Le contrat d'accès et d'utilisation des Services E-Banking est conclu pour une durée indéterminée.

16.1. Résiliation par le Client

Le Client pourra, à tout moment, résilier son accès aux Services E-Banking, sans frais et sans indication de motifs. La résiliation de l'accès par le Client titulaire de compte n'emporte pas de plein droit résiliation des accès conclus avec ses mandataires ou représentants. Par ailleurs, le Client est responsable de la totalité des transactions qui, au moment de la résiliation de l'accès, n'auraient pas encore été inscrites en compte, que ces transactions aient été instruites par lui-même ou son représentant ou mandataire.

La résiliation de l'accès aux Services E-Banking par un mandataire ou représentant n'emporte pas résiliation de l'accès conclu avec le Client titulaire de compte ni, le cas échéant, avec les autres mandataires ou représentants. Le Client titulaire de compte a le droit de résilier l'accès d'un de ses mandataires ou représentants. Dans ces cas, le Client titulaire de compte reste responsable solidairement et indivisiblement pour les opérations effectuées par ce mandataire ou représentant jusqu'à la résiliation de cet accès.

16.2. Résiliation par la Banque

La Banque peut, à tout moment et avec effet immédiat, résilier l'accès du Client aux Services E-Banking, sans frais et sans indication de motifs. Pour le Client consommateur, la Banque peut résilier cet accès moyennant un préavis d'au moins deux mois.

Lorsque la Banque résilie l'accès du Client, elle en informe le Client par tout moyen jugé approprié par la Banque.

Le Client est responsable de la totalité des transactions qui, au moment de la résiliation de l'accès, n'auraient pas encore été portées en compte.

17. Acceptation des conditions générales LuxTrust

Le Client ayant opté pour un mode d'accès LuxTrust déclare avoir pris connaissance et approuver les conditions générales et toutes autres conditions le liant et/ou liant la Banque à LuxTrust dans le cadre de ce mode d'accès (disponibles sur le site www.luxtrust.lu). Le Client ayant opté pour un autre mode d'accès reconnu par LuxTrust, déclare avoir pris connaissance et approuver les conditions générales et toutes autres conditions de son fournisseur le liant et/ou liant la Banque à ce fournisseur dans le cadre de ce mode d'accès.

Annexe :
Avertissement sur les risques inhérents aux virements effectués via les Services E-Banking (banque en ligne)

Avertissement sur les risques inhérents aux virements effectués via les Services E-Banking (banque en ligne)

Cette note vise à informer le Client des risques non exhaustifs liés à l'exécution des virements électroniques.

Le « phishing »

Le « phishing » est une technique utilisée par les escrocs en ligne, consistant à se faire passer pour la Banque avec l'objectif de collecter des données personnelles de clients.

e-mail ou SMS phishing :
Par cette technique, les pirates imitent des messages ou des pages de sites pour recueillir des informations confidentielles relatives à vos comptes bancaires telles que votre numéro de compte ou vos codes d'accès. La victime reçoit un faux e-mail ou SMS d'une banque ou d'un organisme officiel. Ces messages prétextent une mise à jour technique du portail de la banque ou une prétendue vérification de coordonnées personnelles. En cliquant sur un lien contenu dans le message, la victime est alors redirigée vers un site imitant le site officiel de la banque puis invitée à saisir ses identifiants et mots de passe personnels.

Les e-mails peuvent également consister en des e-mails relatifs à des loteries fictives qui annoncent à la victime qu'elle a gagné. Pour percevoir le gain, les escrocs demandent la communication des coordonnées personnelles bancaires.

Certains e-mails sollicitent l'assistance de la victime pour procéder à des transferts de fonds. Une personne demande d'utiliser le compte de la victime pour faire transiter une somme très importante en promettant un pourcentage. Ces sollicitations sont des escroqueries auxquelles il convient de ne pas donner suite.

phone phishing :
Vous recevez un appel téléphonique d'une personne prétendant être un employé de la Banque.

Celui-ci vous annonce que, suite à des problèmes techniques, votre compte va être fermé si vous ne lui communiquez pas vos informations personnelles telles que votre numéro de compte et votre mot de passe.

L'usurpation d'identité

Une personne mal intentionnée utilise sciemment l'identité d'une autre personne dans le but de réaliser des actions frauduleuses.

Pour pouvoir emprunter cette identité, un fraudeur doit avoir préalablement en sa disposition des renseignements personnels et confidentiels qui concernent la victime d'usurpation.

Une usurpation d'identité peut avoir de graves conséquences comme la constitution de faux papiers, l'utilisation de comptes bancaires et la réalisation d'opérations frauduleuses.

Par exemple, en piratant votre adresse e-mail, le fraudeur a accès à tous vos e-mails et peut s'adresser à vos relations en utilisant votre adresse email et votre manière de communiquer et ainsi abuser de la confiance de vos proches.

Le logiciel malveillant

Le logiciel malveillant, appelé « malware » en anglais, est un logiciel développé pour nuire intentionnellement à un système informatique, ou pour en recueillir des données à l'insu de l'utilisateur.

Il en existe de multiples formes : les virus, les vers ou encore les chevaux de Troie en sont les déclinaisons les plus connues (ce virus est installé lorsque vous accédez à un site piraté ou lorsque vous lancez une pièce jointe dans un email ou un SMS ; par exemple, ce virus collecte alors les touches du clavier qui ont été enfoncées en vue de les transmettre automatiquement aux escrocs).

La sophistication de ces logiciels évolue avec l'avancée des technologies.

Que peut-on faire pour réduire les risques ? Revue des bonnes pratiques de sécurité sur Internet

Ne communiquez jamais votre mot de passe ou vos identifiants personnels !

La Banque ne demande jamais de codes d'accès (mot de passe, OTP - One Time Passwords, ou toute autre information confidentielle) à ses clients, que ce soit par email, téléphone, SMS ou tout autre moyen de communication.

Comment protéger votre mot de passe ?

Choisissez un mot de passe sécurisé (composé d'au moins 8 caractères avec des chiffres, des caractères spéciaux, …) et changez-le régulièrement. Utilisez des mots de passe différents pour chaque site que vous consultez (accès à la banque en ligne dans d'autres banques, email, e-commerce, réseaux sociaux, forums, …).

Comment protéger votre appareil ?

Pour protéger votre accès au site E-Banking ou à l'application BL-Mobile, utilisez toujours un appareil de confiance (ordinateur, smartphone, tablette, ou autre) dont vous maîtrisez la sécurité et évitez les ordinateurs publics.

A cet effet, nous vous recommandons :

– d'installer sur votre ordinateur un logiciel antivirus et antispyware mis à jour régulièrement et automatiquement
– d'installer les mises à jour des logiciels récentes de votre système d'exploitation et de votre navigateur Internet
– d'installer uniquement des logiciels de confiance
– d'activer le firewall.

Comment vérifier que vous êtes bien sur le site de banque en ligne de la Banque ?

Accédez directement au site de la Banque en saisissant vous-même l'adresse https://www.banquedeluxembourg.com dans la barre d'adresse de votre navigateur Internet, après avoir vérifié qu'il n'y a pas de faute d'orthographe dans l'adresse, ou depuis vos favoris après avoir enregistré cette adresse au préalable. Ne suivez jamais un lien contenu dans un e-mail ou un SMS.

– Cliquez sur « ACCEDER A MON COMPTE » puis sélectionnez votre mode d'authentification :
– Vérifier que l'adresse commence par « https »
– Vérifier qu'un cadenas est présent en bas et/ou en haut de la page sécurisée et qu'il est fermé
– Double-cliquez sur le cadenas
– Un écran représentant le certificat numérique de la Banque apparaît
– Vérifiez que le nom du certificat comporte bien « BANQUEDELUXEMBOURG.COM ».

Comment vous déconnecter de manière sécurisée et vérifier votre dernière connexion à la banque en ligne ?

Terminez systématiquement toute connexion à votre espace personnel des Services E-Banking en utilisant le bouton « Déconnexion » et fermez la fenêtre de votre navigateur après la consultation de vos comptes en ligne. La date et l'heure de votre dernière connexion réalisée avec vos identifiants sont indiquées sous le bouton DECONNEXION. Pensez également à surveiller les mouvements sur vos comptes.

Comment vous protéger contre le phishing ?

Par cette technique, les pirates informatiques imitent des emails ou des sites institutionnels pour recueillir vos informations confidentielles : numéro de carte de crédit, identifiant, mot de passe, nom, prénom, date de naissance, adresse, numéro de téléphone, etc.

Dans la plupart des cas, cette escroquerie est réalisée par le biais de faux emails des banques ou d'organismes officiels. Ces messages prétextent une mise à jour technique du site correspondant ou une prétendue vérification de vos coordonnées personnelles. En cliquant sur un lien contenu dans l'email, vous êtes alors redirigé vers un site imitant le site institutionnel puis invité à saisir vos informations personnelles.

Pour vous prémunir contre le phishing, étudiez le message ou l'appel, son contenu, l'adresse de l'expéditeur.

Pour rappel, la Banque et toute institution financière en général ne demandent jamais de mot de passe, identifiant ou OTP (One Time Password) par email ou par téléphone à un client.

Que faire si vous avez perdu vos codes d'accès et qui contacter si vous avez une question ?

Si vous avez perdu vos codes d'accès, contactez au plus vite LuxTrust (www.luxtrust.lu) ou le fournisseur de votre moyen d'authentification. Pour toute autre question concernant votre compte et l'accès à l'application BL Mobile Banking, téléphonez à BL-Support au (+352) 26 20 26 30 du lundi au vendredi de 08h00 à 18h00.