

Personnes morales

Contrat de banque à distance neuflizeobc.net

Conditions générales

SOMMAIRE

Article 1 - Objet
Article 2 - Moyens nécessaires - Description et Conditions d'utilisation de la prestation transmission et signature des ordres d'exécution
Article 3 - Règles de sécurité - Opposition pour perte, vol, détournement, utilisation non autorisée de cartes CAP, clé USB, lecteur QR, identifiants ou codes
Article 4 - Adhésion au contrat
Article 5 - Suspension de la prestation assistance téléphonique
Article 6 - Règlement des incidents responsabilité - Force majeure
Article 7 - Tarifs - Facturation et mode de règlement
Article 8 - Preuve des échanges
Article 9 - Dispositions modificatives de la convention de compte
Article 10 - Service Paywebcard

CONDITIONS GÉNÉRALES PAYWEBC@ARD

Article 1 - Service Paywebcard
Article 2 - Fonctionnement du service
Article 3 - Moyens d'authentification - Dispositif de sécurité personnalisé
Article 4 - La délivrance du numéro
Article 5 - Modalité d'utilisation du numéro pour le règlement d'achats de biens et de prestations de services
Article 6 - Blocage du service
Article 7 - Durée de validité du service
Article 8 - Communication de renseignements a des tiers
Article 9 - Conditions financières
Article 10 - Sanctions
Article 11 - Modifications des conditions du contrat
Article 12 - Notifications
Article 13 - Juridiction

Article 11 - Confidentialité des données
Article 12 - Secret Professionnel
Article 13 - Intégralité des accords et modifications du contrat
Article 14 - Durée et résiliation
Article 15 - Evolutions des standards
Article 16 - Cession
Article 17 - Informatique et libertés
Article 18 - Convention de preuve
Article 19 - Droit applicable - Juridique

Sur abonnement la Banque Neuflyze OBC (ci-après « la Banque ») met à la disposition du Client et de ses mandataires utilisateurs (ci-après « les Utilisateurs ») des services internet de Banque en ligne (www.neuflyzeobc.net) permettant aux Clients de la Banque de communiquer, par voie électronique ou télématique pour transmettre des fichiers et/ou des instructions, et accéder à un ensemble de services personnalisés et à des informations de caractère général.

Dans les présentes conditions générales le Client et la Banque sont ci-après individuellement ou collectivement désignés la « Partie » ou les « Parties ».

Le cadre contractuel du présent contrat de banque à distance neuflyzeobc.net se compose des présentes Conditions Générales (« les Conditions Générales ») de la demande d'abonnement et/ou des annexes (ci-après le « Contrat »). La signature de la demande d'abonnement accompagnée des Conditions Générales vaut acceptation des présentes.

ARTICLE 1 - OBJET

Le présent Contrat a pour objet de définir

- ▶ Les conditions et modalités relatives aux échanges entre les Parties, via une liaison Internet par accès au site (www.Neuflyzeobc.net),
- ▶ Les différents types d'instructions ainsi adressées par le Client à la Banque, dans le respect des conditions visées ci-dessus et selon les modalités précisées ci-après,
- ▶ Les modalités de preuve des échanges entre les Parties,
- ▶ Le choix pour l'utilisation des différents services à l'égard des comptes désignés défini :
 - en Annexe 1 – « Liste des Services » et Annexe 2 – « Détail des droits et modes de connexion des Utilisateurs »,
 - Ou dans la demande d'abonnement pour le Service Essentiel.

Toute opération effectuée sur les comptes désignés via le service de Banque en ligne et notamment toute opération de paiement reste régie par les dispositions des conventions de compte courant et convention de services d'investissement et de compte titres applicables à la Banque, à l'exception de celles qui seraient modifiées par le présent Contrat.

Les conditions d'utilisation et les modalités techniques relatives aux échanges de données définies au présent contrat sont ci-après conjointement dénommées « la Prestation ».

ARTICLE 2 – MOYENS NECESSAIRES – DESCRIPTION ET CONDITIONS D'UTILISATION DE LA PRESTATION TRANSMISSION ET SIGNATURE DES ORDRES D'EXECUTION

2.1 MOYENS NECESSAIRES – DESCRIPTION ET CONDITIONS D'UTILISATION DE LA PRESTATION

Le Client fait son affaire personnelle de l'acquisition, de l'installation, de la maintenance de son système informatique et de son raccordement au réseau Internet, du choix d'un navigateur internet compatible permettant l'utilisation du service. Il est tenu de vérifier que l'équipement informatique, le téléphone mobile et la boîte mail utilisés ne contiennent aucun virus ni faille de sécurité et sont en état de fonctionnement, protégés par un pare feu et un antivirus à jour des correctifs de sécurité.

Le Client et la Banque doivent être en possession de l'ensemble des matériels nécessaires à la sécurité.

L'accès au site peut se faire par les moyens d'authentification suivant au choix :

2.1.1. Authentification par clé mobile

L'authentification par clé mobile est un moyen d'authentification fort permettant la connexion des Utilisateurs au site neuflyzeobc.net ainsi que le consentement aux opérations initiées depuis le site neuflyzeobc.net et telles que listées en Annexe 1 « Liste des Services » ou dans la demande d'abonnement pour le Service Essentiel, de façon sécurisée en toute situation de mobilité quel que soit le type d'équipement utilisé (PC, mobile ou tablette).

Procédure d'enregistrement clé mobile

La procédure d'enregistrement décrite ci-après doit être suivie pour chacun des équipements que l'Utilisateur souhaite utiliser pour accéder au service au moyen de la clé mobile :

- ▶ Si l'Utilisateur dispose déjà d'un accès par clavier virtuel, il devra renseigner son identifiant et son code connexion à 8 chiffres. Il recevra ensuite par SMS (sur le numéro de téléphone enregistré dans les systèmes de la Banque) un

code d'activation à usage unique à renseigner également. L'Utilisateur devra enfin choisir son nouveau code PIN à 5 chiffres et le confirmer.

- ▶ Si l'Utilisateur ne dispose pas d'un accès par clavier virtuel mais d'une carte à puce CAP ou d'un certificat numérique X509 sur clé USB, il devra renseigner son identifiant et son mot de passe initial (qu'il pourra récupérer directement sur le site neuflyzeobc.net après s'être authentifié avec sa carte à puce CAP ou son certificat numérique X509 sur clé USB). Il recevra ensuite par SMS (sur le numéro de téléphone enregistré dans les systèmes de la Banque) un code d'activation à usage unique à renseigner également. L'Utilisateur devra enfin choisir son nouveau code PIN à 5 chiffres et le confirmer.
- ▶ Si l'Utilisateur souhaite enregistrer un ou plusieurs nouveaux équipements, il devra renseigner son identifiant et son mot de passe initial (qu'il pourra récupérer directement sur le site neuflyzeobc.net après s'être authentifié directement par clé mobile). Il recevra ensuite par SMS (sur le numéro de téléphone enregistré dans les systèmes de la Banque) un code d'activation à usage unique à renseigner également. L'Utilisateur devra enfin choisir son nouveau code PIN à 5 chiffres et le confirmer.

Le code PIN personnalisé par l'Utilisateur est un authentifiant strictement personnel et confidentiel.

Phase d'utilisation clé mobile

L'Utilisateur pourra ensuite s'authentifier directement depuis tout équipement enregistré sur le site neuflyzeobc.net en saisissant son identifiant directement sur le site neuflyzeobc.net, puis son code PIN à 5 chiffres sur l'application mobile Neuflyze OBC.

L'Utilisateur est informé qu'au bout de cinq saisies consécutives d'un code PIN erroné l'accès au Service depuis l'équipement utilisé est bloqué.

En cas d'oubli ou de compromission de son code PIN, l'Utilisateur est invité à contacter le service d'Assistance Téléphonique.

La Banque attire l'attention du Client et de l'Utilisateur sur le fait qu'en l'absence de numéro de téléphone valide il sera impossible de procéder à l'enregistrement dans le système clé mobile et qu'il appartient en conséquence au Client d'informer la Banque de tout changement de numéro de téléphone mobile ainsi qu'en cas de perte ou de vol du téléphone mobile. En outre, la Banque ne garantit pas l'heure de réception des SMS une fois qu'ils sont pris en charge par un opérateur de téléphonie et n'est pas responsable du décalage éventuel entre la demande d'opération et la réception du SMS.

La Banque attire l'attention du Client déjà Utilisateur du site lors de l'entrée en vigueur des présentes Conditions Générales que son authentification par clavier virtuel ou par carte CAP sera automatiquement désactivée lors du choix de l'authentification par clé mobile. Néanmoins et jusqu'au 14 septembre 2019, date d'entrée en vigueur de la Directive sur les Services de Paiement, dite « DSP 2 », l'authentification par clavier virtuel pourra être réactivée jusqu'à cette date à la demande du Client, aux fins que le Client puisse transmettre son code à un Prestataire de services de Paiement Tiers (PSP Tiers), à l'exclusion de toute autre utilisation. A compter du 14 septembre 2019, le mode d'authentification par clavier virtuel ne sera plus accessible aux Utilisateurs qui devront alors nécessairement opter pour l'authentification par clé mobile telle que définie au présent article, par QR code telle que définie ci-après ou par certificats numériques X509 sur clés USB aux fins de pouvoir continuer à bénéficier des Services de banque à distance.

Consentement aux opérations par clé mobile

Il est expressément convenu qu'afin d'autoriser les opérations initiées depuis le site neuflyzeobc.net et telles que listées en Annexe 1 « Liste des Services » ou dans la demande d'abonnement pour le Service Essentiel, l'Utilisateur manifestera son consentement à ces opérations en saisissant son code PIN personnel et confidentiel sur l'écran de l'équipement utilisé.

2.1.2. Authentification au moyen du système QR Code

L'authentification au moyen du système QR code repose sur l'utilisation d'un lecteur QR pour lequel l'Utilisateur dispose d'un code confidentiel (code PIN défini par l'Utilisateur lors de la première utilisation). Au préalable l'Utilisateur devra activer son lecteur QR en saisissant un code d'activation à usage unique qu'il recevra par SMS, (sur le numéro de téléphone enregistré dans les systèmes de la Banque) ou à défaut par courrier électronique (à l'adresse communiquée par le Client et enregistrée par la Banque dans ses systèmes).

Après avoir saisi son code confidentiel (Code PIN) sur le lecteur, l'Utilisateur peut soit consulter le menu général ou scanner un QR code. Le QR code s'affiche sur le site web neufelizeobc.net après que l'Utilisateur a saisi son identifiant. Après que l'Utilisateur a scanné le QR code, un code à usage unique s'affiche sur le lecteur QR, que l'Utilisateur doit saisir dans le cadre « authentifiant dynamique » s'affichant sur le site web neufelizeobc.net pour s'identifier et accéder au Service.

Les lecteurs QR sont mis à disposition par la Banque.

L'Utilisateur est informé qu'au bout de cinq saisies consécutives d'un code confidentiel (Code PIN) erroné, le lecteur QR est bloqué. Afin de le débloquent l'Utilisateur est invité à contacter le Service d'Assistance Téléphonique.

En cas d'oubli ou de compromission de son code PIN, l'Utilisateur est invité à contacter le service d'Assistance Téléphonique.

La Banque attire l'attention du Client et de l'Utilisateur sur le fait qu'en l'absence de numéro de téléphone ou d'e-mail valides il sera impossible de procéder à l'activation du lecteur QR et qu'il appartient en conséquence au Client d'informer la Banque de tout changement de numéro de téléphone mobile ou d'adresse e-mail ainsi qu'en cas de perte ou de vol du téléphone mobile. En outre, la Banque ne garantit pas l'heure de réception des SMS une fois qu'ils sont pris en charge par un opérateur de téléphonie et n'est pas responsable du décalage éventuel entre la demande d'opération et la réception du SMS.

La Banque peut être amenée pour des raisons techniques, à demander la restitution du lecteur QR détenu par le Client et/ou l'Utilisateur pour l'échanger contre d'autres lecteurs présentant des caractéristiques similaires.

En cas de résiliation du présent Contrat, le Client sera tenu de restituer sans délai le lecteur QR à la Banque.

Il est expressément convenu qu'afin d'autoriser les opérations telles que listées en Annexe 1 « Listes de Services » ou dans la Demande d'abonnement pour le Service Essentiel, l'Utilisateur manifesterà son consentement à ces opérations en scannant le QR code présenté sur le site et en saisissant son code à usage unique généré par le lecteur QR dans le cadre « authentifiant dynamique » s'affichant sur le site internet neufelizeobc.net.

La Banque attire l'attention du Client déjà utilisateur du site lors de l'entrée en vigueur des présentes Conditions Générales que son authentification par clavier virtuel ou par carte CAP sera automatiquement désactivée lors du choix de l'authentification par QR code. Néanmoins et ce jusqu'au 14 septembre 2019, date d'entrée en vigueur de la Directive sur les Services de Paiement, dite « DSP 2 », l'authentification par clavier virtuel pourra être réactivée jusqu'à cette date à la demande du Client, aux fins que le Client puisse transmettre son code à un Prestataire de Services de Paiement Tiers (PSP Tiers), à l'exclusion de toute autre utilisation. A compter du 14 septembre 2019, les modes d'authentification par clavier virtuel et par carte CAP ne seront plus accessibles aux Utilisateurs, qui devront alors nécessairement opter pour l'authentification par clé mobile telle que définie à l'article précédent, par QR code telle que définie dans le présent article, ou par certificats numériques X509 sur clés USB tels que définis ci-après aux fins de pouvoir continuer à bénéficier des Services de banque à distance.

2.1.3. Authentification par Certificats numériques X509 sur clé USB

L'authentification par Certificats numériques X509 sur Clé USB délivrés par une autorité de certification reconnue par la Banque. L'authentification se fait par utilisation du certificat et saisie du code PIN de la clé USB personnel de l'Utilisateur.

Ces certificats permettent de renforcer la sécurité de ces échanges, tant au niveau du transport que de l'envoi des ordres d'exécution, au moyen d'une signature électronique non répudiable par l'une quelconque des parties garantissant, de convention expresse, l'authentification de ces dernières et le contrôle de l'intégrité des données transmises. Cette signature électronique vaut ordre d'exécution dans les conditions stipulées à l'article 2.2 du présent contrat.

2.1.4. Authentification par clavier virtuel (non disponible à compter du 15 mai 2019)

L'authentification par clavier virtuel donne uniquement accès aux services de consultation, aux services d'actualité et d'information générale et à la saisie d'opérations en fonction des services souscrits. Elle est réalisée par l'utilisation d'un

« Identifiant » et d'un « code de connexion » strictement personnels qui doivent être composés sur un clavier virtuel et qui sont adressés par la Banque sous plis séparés au moment de la souscription du contrat. Ce code de connexion initial est un code provisoire que le Client devra modifier lors de son premier accès et ensuite changer régulièrement.

Le Client est informé qu'au bout de trois saisies consécutives d'un code de connexion erroné l'accès au service de Banque en ligne est désactivé.

En cas d'oubli de l'identifiant ou du code de connexion, le Client est invité à contacter le service d'assistance téléphonique.

L'attention du Client est attirée sur le fait que le mode d'authentification par clavier virtuel reste accessible jusqu'au 14 septembre 2019, date d'entrée en vigueur de la Directive sur les Services de paiement, dite « DSP 2 », uniquement aux clients qui sont déjà Utilisateurs au moment de l'entrée en vigueur des présentes conditions générales, et qui n'auront pas à cette date fait le choix de l'authentification par clé mobile telle que définie ci-après ou par QR code telle que définie ci-avant. A compter du 14 septembre 2019, le mode d'authentification par clavier virtuel ne sera plus accessible aux Utilisateurs, qui devront alors nécessairement opter pour l'authentification par clé mobile telle que définie ci-avant ou par QR code telle que définie ci-avant ou par certificats numériques X509 sur clés USB aux fins de pouvoir continuer à bénéficier des Services de banque à distance.

2.1.5. Authentification par Carte à puce CAP (non disponible à compter du 15 mai 2019)

L'authentification par Carte CAP se fait par utilisation dans un lecteur d'une Carte à puce sécurisée CAP pour laquelle l'Utilisateur dispose d'un code confidentiel (code PIN). Après avoir choisi la fonction « CODE » et saisi son code confidentiel (code PIN) sur le lecteur, ce dernier affiche un mot de passe à usage unique à huit chiffres qui permet l'authentification sur le site de Banque en ligne. L'Utilisateur est informé qu'au bout de trois tentatives consécutives d'utilisation de la carte à puce à partir d'un code confidentiel erroné, la carte à puce est définitivement invalidée.

L'attention du Client est attirée sur le fait que le mode d'authentification par carte à puce CAP reste accessible jusqu'au 14 septembre 2019, date d'entrée en vigueur de la Directive sur les Services de Paiement, dite « DSP 2 », uniquement aux clients qui sont déjà Utilisateurs au moment de l'entrée en vigueur des présentes conditions générales, et qui n'auront pas à cette date fait le choix de l'authentification par clé mobile telle que définie ci-avant ou par QR code telle que définie ci-avant. A compter du 14 septembre 2019, le mode d'authentification par carte à puce CAP ne sera plus accessible aux Utilisateurs, qui devront nécessairement opter pour l'authentification par clé mobile telle que définie ci-avant ou par certificats numériques X509 sur clés USB aux fins de pouvoir continuer à bénéficier des Services de Banque à distance.

2.1.6. Commande de cartes à puce CAP ou de Certificats numériques X509 sur clés USB ou de lecteur QR

Les cartes à puce CAP et les lecteurs sont commandés par le Client par l'intermédiaire de la Banque qui les met à disposition des Utilisateurs désignés par le Client.

Les lecteurs QR sont commandés par le Client par l'intermédiaire de la Banque qui les met à disposition des Utilisateurs désignés par le Client.

Pour les certificats, le Client doit effectuer une commande auprès d'une autorité de certification agréée par la Banque.

Le Client choisit l'autorité de certification dans la liste des autorités agréées et communiquée par la Banque sur le site. L'autorité de Certification choisie par le Client fournira le support nécessaire à l'initialisation et l'utilisation du certificat (clé USB, carte).

L'autorité de certification retenue par le Client communiquera à ce dernier sa politique de certification, notamment en matière de durée de validité des certificats numériques. Il est de la responsabilité du Client de renouveler à l'échéance les certificats auprès de l'autorité de certification et de communiquer les éléments nécessaires à la Banque à chaque renouvellement.

Dans le cas où la Banque ne serait pas informée des modifications à l'échéance des certificats, les pouvoirs et les attributs attachés aux certificats concernés ne pourront pas être renouvelés. La Banque ne pourra alors être tenue responsable de la suspension de l'accès aux services.

Paraphe
du Client

Les cartes ou les clés USB que le Client pourrait déjà détenir auprès d'une des autorités de certification agréées par la Banque devront être portées à la connaissance de la Banque dans l'Annexe 2 « Détail des droits et modes de connexion des Utilisateurs ».

L'autorité de certification ou la Banque peuvent être amenées, pour des raisons techniques, à demander la restitution des cartes à puce CAP, certificats ou des clés USB détenues par le Client pour les échanger contre d'autres cartes, certificats ou clés USB à microprocesseur présentant des caractéristiques similaires.

2.2 TRANSMISSION ET SIGNATURE DES ORDRES D'EXÉCUTION - HABILITATIONS

Les ordres d'exécution seront émis sur le site de Banque en ligne avec confirmation de l'ordre par la signature électronique par internet sur le site de Banque en ligne.

La Banque n'exécute les ordres du Client relatifs aux services souscrits dans le cadre des présentes que pour autant :

- ▶ D'une part que les fichiers télétransmis soient exploitables,
- ▶ Et d'autre part qu'elle soit au minimum en possession de l'ordre de validation de chacune des remises que ceux-ci comportent.

Dans ce cadre, la Banque fournira au Client un accusé de réception horodaté.

Dans tous les cas, le Client a seul l'initiative de la communication avec la Banque.

Les transferts d'instructions ou fichiers de remise sécurisés et authentifiés par un Utilisateur autorisé au transfert (« remettant »), et d'autre part les ordres d'exécution signés par un Utilisateur autorisé à signer l'ordre d'exécution (« signataire ») par la signature électronique par internet sur le site de Banque en ligne seront traités par la Banque selon les modalités décrites sur le site et conformément aux heures limites de réception des ordres indiquées dans les Conditions de Tarification en vigueur à la Banque.

Conformément à la réglementation, lors de toute habilitation d'une personne autorisée à remettre ou signer des ordres d'exécution, la Banque demandera la production, de la demande d'abonnement pour le service Essentiel et dans les autres cas de l'Annexe 2 – Détail des droits et modes de connexion des Utilisateurs justifiant des pouvoirs des personnes habilitées sur les comptes désignés, et de leurs justificatifs d'identité. Il est de la responsabilité du Client de s'assurer du domicile de ces mandataires éventuels ce que le Client reconnaît. Il appartient au Client de mettre à jour les habilitations ainsi conférées et d'en informer la Banque dans les meilleurs délais.

Le Client est informé que le fait d'autoriser une personne à agir en tant que signataire permet à ce dernier d'effectuer toute opération choisie par le Client conformément à la demande d'abonnement pour le Service Essentiel ou dans les autres cas conformément à l'Annexe 2 - Détail des droits et modes de connexion des Utilisateurs et vaut délégation de pouvoir et octroi d'un pouvoir spécifique, dérogatoire ou non, à ceux qui ont pu ou pourront être conférés et déposés à la Banque par ailleurs.

Il est expressément convenu que la première utilisation de la carte CAP, clé mobile, QR Code ou du certificat par un Utilisateur vaut acceptation par ce dernier de ces conditions d'utilisation et des termes du présent Contrat.

La Banque recommande que la saisie d'un ordre d'exécution et sa signature soient de préférence effectuées par deux personnes distinctes même s'il est possible techniquement que les fonctions de remettant et signataire soient assumées par une seule et même personne.

Il découle naturellement de la procédure ci-dessus que ce système déroge à tout autre système de contrôle relatif aux pouvoirs. La Banque traitera les opérations ainsi authentifiées sans ajouter aucun contrôle sur le montant des ordres, des remises ou des fichiers qui ne serait pas prévu à la demande d'abonnement pour le Service Essentiel ou dans les autres cas en Annexe 2 - Détail des droits et modes de connexion des Utilisateurs.

En tout état de cause, le Client s'assurera préalablement à chaque échange que les comptes et les Services effectivement utilisés coïncident avec ceux mentionnés expressément dans les pouvoirs bancaires en vigueur délégués par celle-ci, à défaut de quoi les services d'ordres de paiement ne seront pas exécutés et les services de restitution ne pourront être fournis.

Il est également convenu que toute modification du périmètre relatif aux Services ou aux comptes enregistrés sera centralisée par le Client et, de ce fait, communiquée à la Banque par le Client conformément aux procédures définies dans les annexes.

Les opérations ci-dessus ainsi signées seront valablement autorisées, le Client étant engagé par toute utilisation du certificat, de la carte, de la clé USB, clé mobile ou du QR code sauf opposition dans le respect de la procédure décrite à l'article 3.

Comme précisé à l'article 9 ce système permettant de sécuriser la transmission d'ordres d'exécution, le Client ne pourra utiliser le fax pour confirmer ses transferts ou saisies que dans le cas où il est dans l'impossibilité de signer sur le site de Banque en ligne. Etant donné que cette procédure dégrade la sécurité des transferts et saisies d'ordres, elle ne saurait être utilisée que dans le strict cadre d'une procédure de secours. Le Client assumera alors toutes les conséquences liées aux risques inhérents à la confirmation par fax.

Les transferts ou saisies d'ordres en ligne à l'aide du protocole Internet par le Client seront systématiquement chiffrés par la Banque à l'aide de Certificat SSL. Ce chiffrement à l'aide d'une clé de cryptage permet d'assurer la confidentialité des échanges. Il appartient au Client de posséder sur son système informatique les logiciels permettant ce niveau de protection.

Les saisies d'ordres sur Internet doivent être confirmés à la Banque par le Client par des ordres d'exécution.

Dans le cadre de l'utilisation des cartes CAP, la signature des ordres se fait par utilisation de la fonction « Signature » du lecteur sur lequel sera saisi le code « DEFI » fourni sur le site lors de la saisie de l'opération. Le lecteur lui fournira alors un code (« SIGNATURE ») qui devra être saisi sur le site avant de valider l'opération.

Dans le cadre de l'utilisation des certificats numériques X 509, les ordres d'exécution correspondant aux fichiers transmis par les « remettants » habilités du Client doivent être signés par le ou les « signataires » du Client conformément aux Droits des Utilisateurs définis en Annexe 2, qui lors de la demande de signature électronique choisira le certificat à utiliser, acceptera la demande de signature puis validera l'ordre d'exécution.

Dans le cadre de l'utilisation de la clé mobile, la signature des ordres se fait en saisissant son code PIN personnel et confidentiel sur l'écran de l'équipement sur lequel la clé mobile a été activée.

Dans le cadre de l'utilisation du QR code, la signature des ordres se fait en scannant le QR code présenté sur le site à l'aide du lecteur QR et en saisissant son code à usage unique généré par le lecteur QR dans le cadre « authentifiant dynamique » s'affichant sur le site internet neuflyzeobc.net.

ARTICLE 3 – REGLES DE SECURITE – OPPOSITION POUR PERTE, VOL, DETOURNEMENT, UTILISATION NON AUTORISÉE DE CARTE CAP, CLÉ USB, LECTEUR QR, IDENTIFIANTS OU CODES

3.1 RÈGLES DE SÉCURITÉ

Le Client est responsable de la garde, de la conservation et de la confidentialité des identifiants, codes délivrés ou communiqués par la Banque ou code personnalisés par le Client et l'Utilisateur, certificats et de l'utilisation des cartes CAP, des clés USB ou des lecteurs QR ainsi que de la confidentialité des codes qui y sont associés, utilisés dans le cadre de la Prestation.

Le Client répond de ses salariés, collaborateurs et mandataires comme de lui-même et à ce titre est chargé de leur communiquer les termes du présent Contrat et de s'assurer du respect des nécessaires règles de sécurité applicable.

Il appartient au Client de s'assurer notamment :

- ▶ De l'adéquation à ses besoins du Service et des caractéristiques de l'abonnement ;
- ▶ De l'exactitude des informations saisies lors de l'utilisation du Service ;
- ▶ De disposer de la compétence et des moyens nécessaires pour utiliser le Service ainsi que pour accéder et exploiter les informations contenues dans ce Service ;
- ▶ De s'assurer, lors de l'accès au Service, d'être sur le site de banque en ligne de la Banque ;
- ▶ De la fourniture d'une adresse mail valide ;
- ▶ De disposer, avant toute décision et/ou consultation, de l'information à jour du serveur et non de celle stockée sur sa configuration informatique ;

- ▶ De veiller à assurer la confidentialité et la sécurité des informations obtenues par le Service et notamment, de s'assurer du respect de cette confidentialité lors de tout enregistrement, quel que soit le support de cet enregistrement, à savoir disque dur, CD-ROM, DVD, clé USB ..., mais également lors de toute impression ou téléchargement.

Le Client devra prendre connaissance des informations relatives à la sécurité mises à sa disposition sur le site de la Banque.

Le Client est informé des risques inhérents à l'utilisation du réseau Internet, et particulièrement, en termes de :

- ▶ Moindre niveau de sécurité dans la transmission des données,
- ▶ Continuité non garantie par la Banque, dans l'accès au Service, et notamment fermeture du Service, en cas de maintenance du site et/ou problème grave lié au réseau Internet,
- ▶ Rapidité et exécution dans la transmission des données et des mises à jour, non garanties par la Banque,
- ▶ Mise à jour différée des informations relatives aux informations bancaires ou des comptes bancaires, des relevés en ligne ou de l'ensemble des informations communiquées par la Banque, dans le cadre du Service.

Le Client doit tenir compte des menaces et risques significatifs liés au téléchargement de logiciels sur internet, s'il ne peut être raisonnablement certain que le logiciel est authentique et qu'il n'a pas été altéré.

L'attention du Client est attirée sur le fait qu'il ne doit jamais communiquer à quiconque ses codes d'accès ou codes affichés sur le lecteur de carte CAP, lecteur QR, et ce même à la Banque.

Le Client précise à la Banque les autorisations attachées aux différents moyens d'authentification ainsi que l'identité et les coordonnées complètes des Utilisateurs. Il appartient au Client de notifier à la Banque toute modification ou annulation d'attributs et de pouvoirs.

Il appartient au Client de rappeler aux Utilisateurs que les moyens d'authentification, lecteurs QR, cartes à puce CAP, les clés USB, identifiants, codes délivrés ou communiqués par la Banque ou codes personnalisés par l'Utilisateur sont rigoureusement personnels. Chaque Utilisateur doit prendre les mesures nécessaires que ce soit dans le cadre de leur conservation, du transfert ou de la saisie des opérations pour en préserver la confidentialité et les utiliser conformément aux finalités spécifiées aux présentes.

Le Client assume les conséquences de leur divulgation ou utilisation frauduleuse par un tiers en cas de défaillance de sa part à ce titre.

Le Client reconnaît avoir pris connaissance de la politique de sécurité de l'autorité de certification qu'il a retenue.

En cas de résiliation du contrat, le Client ne sera pas tenu de restituer à la Banque, et pourra continuer à utiliser les cartes (à l'exclusion des cartes CAP et lecteurs QR), les clés USB et les certificats numériques pour ses autres besoins. Les cartes CAP et les lecteurs QR devront être restitués à la Banque.

En tout état de cause, à compter du jour où la Banque aura pris connaissance de la résiliation d'un Utilisateur ou du présent Contrat telle que notifiée par écrit par le Client, les signatures électroniques données par les clés mobiles, les cartes CAP, les lecteurs QR ou les clés USB ne vaudront plus ordre d'exécution et la Banque mettra ces cartes CAP, lecteurs QR, clés mobiles en opposition et annulera tous les attributs rattachés aux certificats.

Le Client peut faire usage des clés USB délivrées dans le cadre de son Contrat à d'autres fins que celles décrites dans le présent contrat.

3.2 OPPOSITION POUR PERTE, VOL, DÉTOURNEMENT, UTILISATION NON AUTORISÉE DE CARTES CAP, LECTEURS QR, CLÉS USB, IDENTIFIANTS, OU CODES

Le Client s'engage à signaler à la Banque toute perte ou usage abusif des identifiants et codes dans les plus brefs délais et par tous moyens, et de confirmer sans délai à la Banque cette perte ou cet usage abusif par lettre recommandée avec accusé de réception.

Dès qu'il a connaissance de la perte, du vol, du détournement ou de tout autre utilisation frauduleuse de ses moyens d'authentification (lecteurs QR, carte à

puce CAP, téléphone mobile, tablette, identifiants, codes délivrés par la Banque ou codes personnalisés par le Client, clé USB et/ou des données qui leur sont liées) qu'il utilise auprès de la Banque pour les codes, lecteurs et cartes et auprès des autorités de certification pour clés USB, le Client doit le déclarer à la Banque le plus vite possible aux fins de blocage du moyen d'authentification considéré en indiquant les motifs du blocage. Cette demande d'opposition doit être effectuée conformément aux informations de la Banque disponibles notamment sur le site internet neufilizeobc.net (Assistance>perte moyens d'authentification/de connexion)

Cette déclaration se fera dans un premier temps par tous moyens, puis elle sera immédiatement confirmée par lettre recommandée avec avis de réception. Elle sera prise en compte par l'autorité de certification conformément aux dispositions du contrat entre le Client et cette autorité. La responsabilité de la Banque ne pourra être engagée en cas de manquement aux obligations contractuelles de l'autorité de certification.

En cas d'oubli ou de divulgation du code associé au clavier virtuel, clé mobile, à la carte CAP, à la clé USB ou au lecteur QR, ils doivent faire l'objet d'un remplacement ou de déblocage selon le cas.

Tout code, carte ou clé USB ayant fait l'objet d'une opposition est définitivement inutilisable.

Le Client est informé qu'au bout de trois tentatives consécutives d'utilisation de la carte CAP ou de la clé USB à partir d'un code erroné, la carte ou la clé USB est définitivement invalidée.

Les frais afférents au remplacement de la carte, de la clé USB ou du lecteur QR sont à la charge du Client.

Les dispositions de la convention de compte courant relatives à la responsabilité pour opérations non autorisées seront applicables.

ARTICLE 4 – ADHESION AU CONTRAT

Toute société dont le Client possède le contrôle effectif au sens de l'article 233-3 du code de commerce ou contrôlée par une même société que celle contrôlant le Client aura la possibilité d'adhérer au présent Contrat.

La demande d'adhésion par la nouvelle société adhérente devra être envoyée à la Banque et comporter la signature du Client et l'acceptation par la nouvelle société adhérente de l'ensemble des dispositions du présent contrat selon modèle figurant le cas échéant en Annexe 4.

Par la demande d'adhésion la nouvelle société adhérente donne pouvoir au Client d'intervenir au titre des comptes de la nouvelle société adhérente, le Client étant alors habilitée à déléguer les pouvoirs ainsi conférés sur ces comptes dans les conditions définies à l'article 2.3 habilitations.

Le Client s'engage à informer immédiatement la Banque de toute modification des liens qui l'unissent avec la/ les Société(s) devenue(s) partie(s) au contrat. Dans l'hypothèse où une ou plusieurs des Sociétés ne serait(en) plus contrôlée(s) directement ou indirectement par le Client ou par la société contrôlant le Client, et à condition que la Banque ait bien été informée de cet événement, il sera mis fin à l'adhésion de la (les) dite(s) Société(s) qui ne sera(ont) plus partie(s) au contrat. Il appartiendra au Client de prendre toutes dispositions afin que les habilitations des bénéficiaires désignés concernés par la cessation d'adhésion soient supprimées et que la Banque en soit dûment informée.

Cet article ne s'applique pas au Service Essentiel.

ARTICLE 5 – SUSPENSION DE LA PRESTATION – ASSISTANCE TELEPHONIQUE

La Banque s'engage à maintenir en état de fonctionnement l'ensemble de ses moyens nécessaires à l'exécution du Contrat, chaque jour ouvré, à l'exception des périodes de maintenance indispensables, programmées et notifiées préalablement au Client. Les périodes de maintenance interviendront aux heures où elles entraînent le moins de perturbation pour le Client.

Pour préserver la sécurité et l'intégrité des systèmes, la Banque pourra suspendre l'exécution de la Prestation, sous réserve d'en informer le Client dès que possible et par tout moyen écrit, en cas d'actes ou menaces d'actes de piratage, de malveillance ou de fraude, y compris en ce qui concerne l'accès à la plateforme informatique de la Banque.

Pendant toute la durée de la suspension, les procédures de substitution relatives aux échanges et définies entre les parties définies ci-après s'appliqueront.

TRANSMISSION - Client => Banque

Dans le cas où il est techniquement impossible pour le Client de télétransmettre les opérations, et après que le Client ait refait une tentative de connexion, une procédure de back up sera mise en place.

Avant de mettre en œuvre cette procédure, il conviendra de prendre contact avec l'Assistance Technique de la Banque afin d'optimiser la procédure de back up.

Le Client pourra envoyer ses instructions par fax en indiquant le détail des opérations à l'adresse suivante : Banque Neufilize OBC – 3, avenue Hoche – 75008 PARIS, aux services indiqués ci-après selon les « Modalités de traitement des instructions et horaires d'ouverture des services » figurant en annexe 3.

Nous vous demandons de transmettre par télécopie l'envoi de vos opérations à :

• Type d'opération : Virement Prélèvements

Fax : 01.56.21.97.40

Service : Pilotage Virements et Prélèvements

• Type d'opération : LCR BAPL

Fax : 01.56.21.72.20

Service : Portefeuille

• Type d'opération : TLMC

Fax : 01.56.21.77.60

Service : Chèques

Données obligatoires à indiquer sur la télécopie :

- Nom de votre société
- Numéro du compte
- Montant total
- Nombre d'opérations
- Signature autorisée

Dans ce cas, hors pouvoirs spécifiques, les contrôles effectués seront liés à la procédure de substitution utilisée. La Banque vérifiera notamment si les signataires sont autorisés à signer ce type d'instruction selon les pouvoirs déposés à la Banque.

RECEPTION - BANQUE => CLIENT

Dans le cas où le Client ne parvient pas à récupérer les informations fournies par la Banque, et après que le Client ait refait une tentative de connexion, une procédure de back up sera mise en place.

Avant de mettre en œuvre cette procédure, il conviendra de prendre contact avec l'Assistance Technique de la Banque afin d'optimiser la procédure de back up.

Le Client pourra demander à la Banque la récupération des éléments comptables par fax ou téléphone.

Si, passé un délai de trente (30) jours calendaires à compter de la notification de la suspension, l'exécution de la Prestation est toujours suspendue, le présent contrat pourra être résilié sans préavis par le Client moyennant l'envoi à la Banque d'un courrier en recommandé avec avis de réception, à l'adresse mentionnée à l'Annexe 5 Contacts & paramètres ou pour le service Essentiel dans la demande d'abonnement.

La Banque s'efforcera de fournir au Client, la meilleure disponibilité des Services de Banque en ligne et PaywebCard, sauf cas de force majeure, panne ou maintenance.

Cette garantie ne saurait s'entendre d'une garantie absolue, en termes de disponibilité ou de performances, compte tenu de la structure du réseau Internet et des spécificités liées au Service sur Internet.

La Banque pourra interrompre le Service pour des raisons de maintenance à des heures de basse fréquentation déterminées en fonction des statistiques de connexion, et ne pourra être tenue pour responsable des conséquences des interruptions.

En cas d'interruption du Service pour quelque cause que ce soit conduisant à l'impossibilité de signer sur le site de Banque en ligne le Client demeure libre d'effectuer ses

opérations en s'adressant à son Banquier par d'autres moyens de communication, tels que le téléphone ou le fax. Etant donné que cette procédure dégrade la sécurité des transferts et saisies d'ordres, elle ne saurait être utilisée que dans le strict cadre d'une procédure de secours. Le Client assumera alors toutes les conséquences liées aux risques inhérents à la confirmation par fax.

Le Client reconnaît avoir été informé qu'il a la possibilité de bénéficier pour tout problème technique d'un service téléphonique d'assistance dont le n° est rappelé sur la page d'accueil du site.

ARTICLE 6 – REGLEMENT DES INCIDENTS – RESPONSABILITE – FORCE MAJEURE

6.1 RÈGLEMENT DES INCIDENTS

En cas de constatation d'un défaut quelconque de fonctionnement technique, chaque Partie s'engage à en aviser l'autre par tous moyens et dans les meilleurs délais, à en relever les éléments, à favoriser la recherche des causes et à collaborer avec l'autre le plus complètement possible à l'effet d'y remédier.

Pendant le délai nécessaire à la disparition du défaut, les Parties étudieront les procédures de substitution pouvant être mises en place.

Dans le cas de contestation, les parties désigneront d'un commun accord un expert qui procédera à l'analyse des fichiers de preuves concernés. A défaut d'accord, compétence est attribuée au Président du Tribunal de Commerce de Paris pour effectuer cette désignation. Les parties seront liées par la décision de l'expert.

6.2 RESPONSABILITE

Les obligations de la Banque sont des obligations de moyens.

Ainsi, la Banque n'est responsable de l'exécution défectueuse d'une de ses obligations qu'autant que celle-ci est due à sa faute, sa négligence ou à un quelconque manquement à ses obligations contractuelles.

Aucune Partie ne peut engager la responsabilité de l'autre en cas de dysfonctionnement imputable à un tiers.

Seuls les dommages directs subis par une Partie pourront être indemnisés par l'autre Partie, les dommages indirects et notamment les pertes de revenus, d'activité, d'un contrat, d'économies ou de bénéfices escomptés, ne pouvant en aucun cas engager la responsabilité d'une des Parties.

Dans l'hypothèse où l'une des Parties aurait recours à un ou des sous-traitants, pour traiter une partie de la Prestation au titre du présent contrat, elle restera pleinement et entièrement responsable de la réalisation et de la bonne fin des prestations sous-traitées et fera respecter sous sa seule responsabilité par le ou les sous-traitants toutes les stipulations du présent contrat.

D'une manière générale, les Parties garantissent que l'exécution de leurs obligations contractuelles ne contrevient à aucune disposition légale ou réglementaire qui leur serait applicable.

Sous peine d'irrecevabilité, toute réclamation concernant la transmission d'un fichier ou la récupération des informations sur le site de la Banque doit être formulée dans un délai de 13 mois.

6.3 FORCE MAJEURE

Dans tous les cas, la responsabilité de la Banque ne sera pas engagée du fait du retard ou de la défaillance dans la fourniture de la Prestation tenant à un cas de force majeure, notamment, tout événement irrésistible et extérieur aux Parties, par exemple :

- ▶ Le défaut de fourniture de courant électrique,
- ▶ Les interventions administratives ou législatives,
- ▶ Les contingences techniques, administratives ou autres, intéressant les lignes et les réseaux de transmission, Les guerres ou menaces de guerre, terrorisme, sabotage, émeutes, grèves externes, incendies, inondations.

En pareil cas, chaque Partie informera l'autre Partie de la survenance de tels événements dès que possible. Elles définiront alors ensemble la procédure de substitution à mettre en œuvre.

ARTICLE 7 – TARIFS - FACTURATION ET MODE DE REGLEMENT

Les tarifs, leur révision, ainsi que les modalités de facturation et de règlement relatifs à la Prestation réalisée au titre des présentes sont indiqués en Annexe 3 du présent contrat ou dans la demande d'abonnement Essentiel, étant précisé qu'en cas d'adhésion au contrat d'une société contrôlée, chaque société sera facturée au titre du contrat (dans ce cas, la facturation sera effectuée de façon globale sur le compte désigné en annexe 3 comme "compte à débiter") sauf option contraire aux termes de cette même annexe.

Le Client autorise expressément et irrévocablement la Banque à prélever mensuellement sur le compte ainsi désigné le montant des sommes dues.

ARTICLE 8 – PREUVE DES ECHANGES

Le Client et la Banque reconnaissent que les instructions, et notamment les ordres de virement transmis et signés à l'aide de Certificat X509, de lecteur QR, clé mobile ou de cartes à puce dans le respect des conditions décrites aux présentes, ont la valeur de documents originaux les liant d'une manière pleine et entière. En conséquence, les parties entendent leur attribuer une valeur probatoire. La portée de la preuve est celle accordée à un original, au sens d'un document écrit, signé de manière manuscrite.

Lorsque le Client nie avoir donné son consentement pour réaliser une opération, il appartient à la Banque d'apporter la preuve que l'opération a été authentifiée, dûment enregistrée et comptabilisée et qu'elle n'a pas été affectée par une déficience technique. Cette preuve peut être apportée par tous moyens, notamment à ce titre les registres informatisés, les documents conservés dans les systèmes informatiques de la Banque dans des conditions raisonnables de sécurité conformément aux normes de la profession, seront utilisés comme les preuves des transactions, des échanges, des documents et des données consultés ou envoyés, dans le cadre du Service. L'archivage et l'enregistrement des données sont effectués sur un support fiable et durable de manière à correspondre à une copie fidèle et durable conformément à la réglementation applicable.

ARTICLE 9 – DISPOSITIONS MODIFICATIVES DE LA CONVENTION DE COMPTE

Les dispositions de la convention de compte qui ne sont pas modifiées par les présentes sont applicables notamment quant aux opérations de paiement émises sur le service étant précisé que par dérogation à la convention de compte les ordres de virement devront être systématiquement saisis et confirmés sur le site à l'exclusion de tout autre mode de communication réserve faite des procédures de secours.

9.1 INSTRUMENTS FINANCIERS ÉLIGIBLES À LA TRANSMISSION D'ORDRES

Nonobstant les dispositions relatives aux titres et instruments financiers pouvant faire l'objet d'une inscription en compte en application de la Convention de Compte, la transmission d'ordres de bourse par l'intermédiaire du Service sera limitée aux titres et instruments financiers et aux marchés suivants, pour autant qu'ils soient des instruments financiers « non complexes », tels que définis dans les Conditions Générales de la Convention de Compte :

- ▶ Instruments financiers admis aux négociations sur le marché réglementé de la Bourse de Paris, à l'exclusion des opérations sur les marchés dérivés réglementés ou de gré à gré et des EMTN (Euro Medium Term Notes).
- ▶ Instruments financiers admis aux négociations sur les marchés réglementés des Bourses étrangères suivantes : Allemagne, Autriche, Belgique, Danemark, Espagne, Etats-Unis (NYSE, NASDAQ), Finlande (avec restrictions), Grande Bretagne, Irlande, Italie, Luxembourg, Norvège, Pays-Bas, Portugal, Suède (avec restrictions), Suisse, à l'exclusion des opérations sur les marchés dérivés réglementés ou de gré à gré et des EMTN (Euro Medium Term Notes).
- ▶ OPCVM dont la Banque assure la commercialisation et figurant sur le Site (à l'exclusion des OPCVM structurés).

9.2 CONDITIONS DE FOURNITURE DES SERVICES D'INVESTISSEMENTS PAR LA BANQUE

L'initiative des ordres transmis par l'intermédiaire du

service appartient au Client et il déclare en assumer la responsabilité.

Il appartient au Client avant toute décision d'investissement transmise par l'intermédiaire du service, d'apprécier si compte tenu des informations dont il dispose ou qui lui ont déjà été fournies, l'instrument financier qu'il envisage de souscrire lui convient, notamment en termes de risques et au regard de sa situation financière ou de ses objectifs.

Dans le cas où il estime ne pas disposer d'informations suffisantes il doit, avant la passation de l'ordre, solliciter des informations complémentaires notamment auprès de la Banque.

A ce titre, le Client reconnaît avoir conscience :

- ▶ Des risques liés aux fluctuations boursières,
- ▶ Que, de façon générale afin de pondérer ces risques il est nécessaire de diversifier ses placements,
- ▶ Que tous les produits financiers comportent un certain degré de risque et que même les stratégies de placement à faible risque comportent un élément d'incertitude

L'accès au Service n'est ouvert ni pour les comptes objets de mandat de gestion, ni pour les comptes objets d'une convention de conseil en investissement.

Dans la mesure où les ordres transmis par l'intermédiaire du Service ne peuvent porter que sur des instruments financiers non complexes, la Banque sera dispensée d'obtenir des informations sur les connaissances et l'expérience du Client et ne sera pas tenue de vérifier si le produit ou service convient au Client, la transmission des ordres étant alors faite aux risques et sous la responsabilité de ce dernier qui ne bénéficiera pas de la protection correspondante des règles de conduite.

Le Client s'engage à ne pas utiliser le Service pour passer des ordres suite à une recommandation qui lui aurait été faite par la Banque dans le cadre d'un service de Conseil en investissement.

Il est recommandé au Client de consulter régulièrement les informations financières publiées sur le site internet de la Banque.

9.3 COUVERTURE DES ORDRES

Conformément aux dispositions de la Convention de Compte le Client s'engage à respecter les règles de couverture minimale applicables en vertu de la réglementation en vigueur.

Les garanties affectées au calcul de la couverture des opérations par l'intermédiaire du Service sont constituées de toutes les sommes et valeurs figurant sur le compte et sont rappelées sur écran, sous forme de couverture disponible, étant précisé que les informations correspondantes se rapportent aux positions constatées la veille. Il appartient au Client de s'assurer qu'il respecte les règles de couverture à tout moment notamment compte tenu des ordres transmis le jour même.

9.4 EXÉCUTION DES ORDRES TRANSMIS PAR LE CLIENT

Le Client doit s'assurer qu'il transmet son ordre dans des conditions permettant son exécution compte tenu des délais d'acheminement et des horaires d'ouverture du marché ou des heures limites de transmission des ordres.

La Banque assume la responsabilité de la bonne exécution de l'ordre après que la confirmation de la prise en compte de l'ordre a été adressée au Client et dès l'instant où ce dernier a confirmé son accord. A cet égard, il est précisé que sur la Bourse Allemande, les ordres doivent être transmis avant 20 heures.

Avant toute souscription d'OPCVM, il appartient au Client de prendre connaissance du Document d'Information Clés pour l'Investisseur (DICI) ou du Document d'Information Clés (DIC) des OPCVM concernés mis à disposition par la Banque sur le site internet.

Si, au moment de la transaction, le DICI/DIC n'est pas immédiatement disponible, la Banque s'engage à le fournir au Client dans les meilleurs délais. Le Client reconnaît expressément que dans ce cas, il pourra au choix consentir à le recevoir postérieurement à la transaction ou reporter celle-ci après l'avoir reçu.

Toute modification ou annulation d'un ordre non encore

exécuté doit être demandée par écrit par le Client à la Banque ; seuls les ordres « à cours limité » non encore exécutés peuvent en principe être modifiables ou annulables sur le Service,

Outre l'avis d'opéré qui est adressé par courrier dans les conditions de la Convention de Compte, le Client est informé de façon générale, du statut de ses ordres et de leur exécution par consultation directe sur le site de la page "carnet d'ordres" ou de la page "portefeuille", sans que cette information puisse être considérée comme se substituant aux avis d'opéré.

9.5 INFORMATIONS SUR L'ACTUALITÉ BOURSIÈRE ET FINANCIÈRE

Les informations mises à disposition sur le site en matière d'actualité boursière et financière sont fournies à titre purement indicatif et ne sauraient constituer la moindre incitation ou recommandation d'investir par la Banque.

Elles sont élaborées à partir de sources que la Banque estime fiables et ne sauraient être garanties par elle (que ce soit au regard de leur exactitude, leur fiabilité ou l'exhaustivité des opinions ou informations) compte tenu, notamment, des délais de mise à jour, de traitement et de contrôle à effectuer.

Elles sont sujettes à modification à tout moment sans notification préalable.

Les performances passées ne préjugent pas des performances futures et ne sont pas constantes dans le temps. De même aucun élément du site ne constitue un conseil financier, juridique, fiscal ou autre ni ne saurait fonder à lui seul une décision de placement ou une autre décision.

La Banque ne saurait être tenue responsable des dommages directs et indirects, tels que pertes financières, manque à gagner, perte quelconque résultant d'une erreur ou d'une information consultée sur le site.

La consultation des informations fournies au Client est exclusivement réservée à son information personnelle. Il s'interdit de les utiliser pour une autre finalité, notamment à destination de tiers pour justifier de son patrimoine.

Toute autre utilisation, notamment commerciale telles que : vente de données, exploitation du Service à d'autres fins est prohibée et ne saurait engager la Banque.

9.6 EXTRAITS DE COMPTE – INFORMATION DU CLIENT

En souscrivant le présent contrat, le Client bénéficie automatiquement de la mise à disposition sur le site de Banque en ligne dans le menu e-documents sous format électronique (en format pdf), des documents suivants : documents d'informations clés (DIC) ou documents d'informations clés pour l'investisseur (DICI), avis d'opérations, avis d'opérations sur titres, avis d'exécution des ordres (avis d'opéré), confirmation d'opération sur instruments dérivés, relevés de comptes titres, extraits de compte, relevés de carte bancaire, imprimés récapitulatifs des opérations sur valeurs mobilières et revenus de capitaux mobiliers (IFU), avis de taxe sur les transactions financières, relevé fiscal de détention des titres.

Le Client sera informé de la mise à disposition de chaque nouveau document d'information relatif aux instruments financiers par voie d'e-mail dans la limite d'un e-mail par jour concernant les avis d'exécution ou relevés de comptes titres étant précisé qu'il n'y aura pas lieu à notification d'avis d'exécution et/ou de relevés de comptes titres lorsqu'il s'agit de comptes faisant l'objet d'un mandat de gestion.

Les autres documents seront mis à disposition sans notification préalable.

Chacun de ces documents sera consultable pendant une période de quatre ans de date à date à compter de sa mise à disposition sur le site à l'exception des avis d'opérations qui ne seront consultables que pendant une période de trois mois à compter de leur mise à disposition.

Par ailleurs le Client pourra également faire une demande à la Banque de lui mettre ces documents à disposition en dehors de l'accès via le site pendant une période de dix ans à compter de leur mise à disposition.

Le Client a la possibilité de demander à recevoir ces documents également sous format papier.

En cas de résiliation du présent contrat, le Client ne pourra plus consulter en ligne ces documents. Il lui appartiendra en conséquence de veiller à les sauvegarder avant la date effective de résiliation.

ARTICLE 10 – SERVICE PAYWEBCARD

Le service PaywebC@rd est ouvert à la demande du Client dans la demande d'abonnement ou en Annexe 1, sous la condition expresse de posséder également une carte bancaire en cours de validité émise par la Banque. Il permet de sécuriser le règlement d'achats à distance auprès de commerçants ou prestataires de services, par carte bancaire par le biais d'internet au moyen de la fourniture d'un ou de plusieurs e-numéros. Les conditions de fonctionnement du service sont soumises aux conditions du contrat porteur Carte Bancaire souscrit par ailleurs par le Client, ainsi qu'aux Conditions Générales de fonctionnement du service PaywebC@rd ci-après.

CONDITIONS GÉNÉRALES PAYWEBC@RD

Le présent contrat a pour objet de fixer les règles de fonctionnement et d'utilisation du service PaywebCard mis à la disposition du titulaire d'une carte bancaire de paiement de la Banque Neuflyze OBC pour régler ses achats à distance en toute confiance.

ARTICLE 1 – SERVICE PAYWEBCARD

Dans un but de sécurisation des achats effectués à distance par carte bancaire, le service PaywebCard (ci-après dénommé le «Service») a pour objet la mise à la disposition du Client (ci-après dénommé le «Client», d'un ou de plusieurs «e-numéros» (ci-après dénommé le «Numéro» ou les «Numéros»), exclusivement destinés) au règlement d'achats à distance, par le biais d'Internet ou de tout autre moyen de communication à distance, de biens ou de prestations de service auprès de commerçants ou prestataires de services, français ou étrangers, ayant adhéré au système de paiement par carte et affichant le logo CB et/ou le logo du réseau international Visa ou Eurocard / Mastercard (ci-après dénommé les «Commerçants» ou le «Commerçant»).

Le Service et le Numéro ne permettent pas :

- ▶ d'obtenir des espèces auprès des établissements de crédit et des institutions financières.
- ▶ De régler, aux commerçants et prestataires de services des achats de biens ou des prestations de services autrement que lors d'achats à distance,
- ▶ De charger ou de recharger un porte-monnaie électronique.

ARTICLE 2 – FONCTIONNEMENT DU SERVICE

2.1 Compte tenu de son objet même, le Service ne peut être souscrit que par des clients de la Banque Neuflyze OBC proposant ce service (ci-après dénommé l'«Émetteur»), titulaires d'un compte et d'une carte de paiement émise par cet Émetteur.

2.2 L'adhésion au Service est automatique lorsque le Client détenteur d'une carte adhérent et est adhérent au service de Banque à Distance «neuflyzeobc.net».

2.3 De manière sécurisée et chiffrée, un Numéro sera attribué par l'Émetteur au Client par le biais du Service, pour la transaction envisagée. Le Numéro ainsi obtenu est lié à la carte bancaire que le Client a choisi pour participer au Service et n'est utilisable que dans le cadre d'un usage défini à l'article 4.

ARTICLE 3 – MOYENS D'AUTHENTIFICATION - DISPOSITIF DE SÉCURITÉ PERSONNALISÉ

Les moyens d'authentification permettant d'accéder au Service sont identiques à ceux utilisés par le Client pour accéder à neuflyzeobc.net.

ARTICLE 4 – LA DÉLIVRANCE DU NUMÉRO

4.1 Le Client s'engage à utiliser le Numéro exclusivement lors de vente à distance sur Internet ou tout autre moyen de communication à distance pour des achats de biens ou des prestations de services auprès de Commerçants acceptant les cartes Visa, CB et/ou Eurocard/Mastercard.

Paraphe
du Client

4.2 Il est recommandé au Client de ne demander un Numéro qu'au moment de réaliser une transaction, auprès d'un Commerçant.

4.3 Lorsque le Numéro a été demandé pour une transaction unique et dans le cas où le Client ne souhaite pas confirmer ou donner suite à la transaction alors que le Numéro lui a été attribué, le Numéro reste valable pendant une durée d'un mois à compter de la demande. Si, à l'expiration de la période de validité susvisée, le Numéro n'a pas été utilisé par le Client, il est détruit par l'Émetteur et ne peut donc être réutilisé par le Client dans le cadre d'une autre transaction, y compris avec le même Commerçant.

Le Client a toutefois la possibilité, via le Service, d'annuler son Numéro non utilisé avant la fin du délai de validité de un mois. Une fois la transaction confirmée par le Client et autorisée/ou mis en recouvrement par le Commerçant, le Numéro est désactivé et ne peut donc être utilisé par le Client dans le cadre d'une autre transaction, y compris avec le même Commerçant.

4.4 L'émetteur se réserve le droit de limiter le nombre de Numéros en possession du Client et non utilisés.

ARTICLE 5 – MODALITÉS D'UTILISATION DU NUMÉRO POUR LE RÈGLEMENT D'ACHATS DE BIENS ET DE PRESTATIONS DE SERVICES

5.1 Le Numéro ne doit être utilisé que pour régler des achats de biens ou de prestations de service réellement effectués.

5.2 L'ordre de paiement donné au moyen du Service et d'un Numéro est irrévocable.

5.3 Les paiements effectués au moyen du Numéro ne sont possibles que dans les limites fixées et notifiées par l'Émetteur pour la carte de paiement du Client. Ces conditions s'ajoutent à celles définies spécifiquement entre le Client et l'Émetteur pour l'utilisation du Service.

5.4 Les paiements par le biais du Service sont effectués selon les conditions et procédures en vigueur chez les Commerçants.

5.5 Les règlements présentés à l'encaissement par les Commerçants sont automatiquement débités du compte sur lequel fonctionne la carte de paiement choisie pour générer le Numéro selon les dispositions convenues entre le titulaire de celui-ci et l'Émetteur auxquelles la présente convention n'apporte aucune novation.

Le montant des transactions réglées au moyen d'un Numéro se cumule avec celui des transactions réglées avec la carte de paiement du Client dans la mesure où elles sont débitées sur le même compte. Le montant de ces transactions vient donc s'imputer sur le plafond négocié entre le Client et l'Émetteur concernant les dépenses réalisées au moyen de ladite carte. Même si ces conventions prévoient un différé de paiement, l'Émetteur a la faculté de débiter immédiatement le compte du montant des dépenses réglées à l'aide d'un Numéro en cas de décès, d'incapacité juridique du Client et/ou du titulaire du compte, d'incidents de paiement ou de fonctionnement du compte, de clôture du compte ou du retrait de la carte de paiement, décision qui serait notifiée au titulaire de la carte de paiement susvisée par simple lettre. De même, l'Émetteur a la faculté de débiter immédiatement le compte du montant des paiements réalisés au moyen de Numéros, si le cumul des transactions de paiement réglées par Numéros et par la carte de paiement dépasse les limites fixées par l'Émetteur.

5.6 Dans la mesure où le Service ne peut être utilisé que dans le cadre de vente à distance par Internet ou tout autre moyen de communication à distance de biens ou de prestations de services ne donnant pas lieu à l'émission de factures signées par le Client ou son mandataire ou assorties du contrôle d'un code confidentiel, le titulaire du compte sur lequel fonctionne le Service autorise l'Émetteur à débiter son compte au vu des enregistrements ou des relevés transmis par le Commerçant. Les réclamations concernant ces opérations sont traitées dans les conditions prévues aux Conditions Générales des cartes bancaires.

5.7 Le Client et/ou le titulaire du compte doit s'assurer que le jour du débit des règlements par le Service, le compte présente un solde suffisant et disponible.

5.8 Sauf exception, le montant détaillé des paiements effectués au moyen du Service passé au débit du compte sur lequel fonctionne le Service figure sur le même relevé des opérations que les opérations réalisées au moyen de la carte de paiement du Client. Le relevé peut également être consulté par voie électronique sur le site neuflyzeobc.net.

5.9 Sur le relevé susvisé, le montant détaillé des paiements effectués au moyen du Service passé au débit du compte sur lequel fonctionne le Service est mentionné comme résultant de transactions réglées au moyen de la carte de paiement du Client. Le relevé de compte est un document à valeur contractuelle, à la différence de l'historique des transactions proposé par le Service.

5.10 L'émetteur reste étranger à tout différend commercial, c'est à dire autre que relatif à l'opération de paiement, pouvant survenir entre le titulaire du Numéro et le Commerçant. L'existence d'un tel différend ne peut en aucun cas justifier le refus du Client et/ou du titulaire du compte sur lequel le Service fonctionne, d'honorer les règlements des transactions réglées au moyen du Service.

Important : Le Service n'est pas utilisable sur certains sites marchands qui exigent la présentation de la carte réelle au retrait de la prestation.

ARTICLE 6 – BLOCAGE DU SERVICE

À la suite de la mise en opposition d'une carte de paiement du Client, à laquelle est adossé le Service il n'est plus possible d'obtenir de nouveaux Numéros sur cette carte de paiement mais néanmoins les Numéros générés antérieurement à la date d'opposition restent valables.

Des frais pour blocage du Service peuvent être perçus par l'Émetteur; Ils sont notifiés suivant les dispositions prévues à l'article 9.

ARTICLE 7 – DURÉE DE VALIDITÉ DU SERVICE

7.1 L'adhésion au Service est conclue pour une durée équivalente à la durée de validité des cartes de paiement enregistrées dans le Service ainsi que pour la durée équivalente de l'abonnement neuflyzeobc.net.

7.2 Le Client ou l'Émetteur peuvent mettre fin au Service à tout moment par lettre recommandée avec accusé de réception avec un préavis d'un mois. Cette disposition ne remet pas en cause le droit de l'Émetteur à mettre fin immédiatement au Service, notamment en cas de comportement répréhensible du Client ou d'anomalie grave de fonctionnement du compte sur lequel fonctionne le Service.

La résiliation ou le non renouvellement du Service n'entraîne pas la résiliation des cartes enregistrées dans le Service.

ARTICLE 8 – COMMUNICATION DE RENSEIGNEMENTS A DES TIERS

- ▶ De convention expresse, l'Émetteur est autorisé à diffuser les informations recueillies dans le cadre du présent contrat ainsi que les informations relatives aux opérations effectuées au moyen d'un Numéro. Ces informations feront l'objet de traitements, automatisés ou non, afin de permettre la gestion du fonctionnement du Service et d'assurer la sécurité des paiements.
- ▶ Les informations recueillies à l'occasion du présent contrat ne seront que pour les seules nécessités de la gestion interne du Service et pour satisfaire aux obligations légales et réglementaires.
- ▶ Pour satisfaire les finalités précisées ci-dessus, les informations en question pourront être communiquées aux établissements de crédit, institutions financières visées à l'article L. 518-1 du Code Monétaire et Financier, aux organismes intervenant dans le cadre de la délivrance et du fonctionnement du Service, à des sous-traitants, aux commerçants ou prestataires de services acceptant le paiement par carte de paiement, ainsi qu'à la Banque de France et au Groupement des Cartes Bancaires.
- ▶ Le Client et/ou le titulaire du compte bénéficie d'un droit d'accès et de rectification des données personnelles le concernant. Il peut exercer ce droit auprès de l'Émetteur.

ARTICLE 9 – CONDITIONS FINANCIÈRES

9.1 Le Service est facturé selon les modalités figurant aux conditions tarifaires définies par l'Émetteur.

9.2 Les conditions financières sont précisées dans le recueil de Tarification Générale applicable aux particuliers et aux professionnels, dans les conditions tarifaires particulières, ou dans tout document approuvé par le Client et/ou le titulaire du compte sur lequel le Service fonctionne et notamment le contrat d'abonnement de Banque à distance neuflizeobc.net.

9.3 Tous les frais sont prélevés sur le compte désigné par le Client dans le contrat de Banque à distance neuflizeobc.net.

ARTICLE 10 – SANCTIONS

Tout usage abusif ou frauduleux du Service ou d'un Numéro est passible des sanctions prévues par la loi. Tous frais et dépenses réels engagés pour le recouvrement forcé des opérations sont à la charge solidairement du Client et/ou du titulaire du compte concerné. Le montant des opérations qui n'aura pas pu être débité au compte sera majoré d'un intérêt dont le taux est celui des débits non autorisés à partir de la date de valeur sans mise en demeure préalable.

ARTICLE 11 – MODIFICATIONS DES CONDITIONS DU CONTRAT

11.1 Modifications non financières :

L'émetteur se réserve le droit d'apporter des modifications non financières aux conditions du contrat qui seront portées à la connaissance du titulaire du compte et/ou du Client, notamment lors du renouvellement de celle-ci. Ces modifications sont applicables :

- ▶ Un mois après leur notification si la carte, en cours de validité, n'est pas restituée à la Banque Neufelize OBC avant l'expiration de ce délai, ou si elle est utilisée après ce délai,
- ▶ Immédiatement lorsqu'elles sont acceptées par le Client au moment du renouvellement du support.

11.2 Modifications financières :

L'émetteur se réserve le droit d'apporter des modifications tarifaires aux Conditions Générales applicables aux particuliers et aux professionnels. Ces modifications seront portées à la connaissance du Client dans les Conditions de Tarification. L'absence de contestation par le titulaire du compte et/ou de la carte dans un délai de deux mois après cette communication vaut acceptation de ces modifications tarifaires.

ARTICLE 12 – NOTIFICATIONS

Hormis les cas où le présent contrat en dispose autrement, toute notification à l'Émetteur relative à la survenance de tout événement prévu par le présent contrat, s'effectuera par lettre recommandée avec accusé de réception adressée à l'Émetteur.

ARTICLE 13 – JURIDICTION

Le présent contrat est soumis à la loi française.

Tout litige découlant du présent contrat ou qui en serait la suite ou la conséquence sera porté devant le Tribunal de Commerce de Paris. Toute action éventuelle du client contre la Banque Neufelize OBC devra, sous peine de forclusion, être exercée dans le délai d'un an de sa cause.

ARTICLE 11 – CONFIDENTIALITE DES DONNEES

Sous réserve de ce qui est dit à l'article 12, chaque Partie s'engage à considérer comme confidentielles, et à ne pas utiliser, les informations qu'elle aura pu recueillir au sujet de l'autre Partie ou de toute Société du Groupe concernée ainsi que toutes informations et documents échangés entre elles dans le cadre du présent contrat. Les Parties s'engagent ainsi à assurer la confidentialité de ces informations et à prendre toutes les mesures nécessaires pour assurer le respect de cette confidentialité par leurs employés, les personnes morales de leurs groupes respectifs et leurs sous-traitants.

Ces obligations de confidentialité et de non utilisation seront levées dans l'hypothèse où les informations et/ou les documents seraient tombés dans le domaine public, sans faute de la Partie qui les a reçus, ou pour faire droit à la demande d'une autorité administrative, judiciaire ou de tutelle dans les conditions définies par la loi.

ARTICLE 12 – SECRET PROFESSIONNEL

Aux termes des dispositions prévues aux articles L 511-33 et L 511-34 du Code Monétaire et Financier, la Banque est tenue par le secret professionnel.

Toutefois, ce secret peut être levé, conformément à la loi, notamment à la demande des autorités de tutelle, de l'administration fiscale ou douanière, du service institué à l'article L 562-4 du code monétaire et financier, ainsi qu'à celle du juge pénal, ou encore en cas de réquisition judiciaire notifiée à la Banque.

Le Client reconnaît être informé que la Banque est susceptible de confier à des tiers, intermédiaires, personnes physiques ou morales, prestataires de services, le traitement de ses opérations, l'exécution de ses ordres, et plus généralement tous travaux pouvant contribuer à la fourniture des prestations prévues dans la présente convention, ou qui pourraient y être rattachées à l'avenir. En conséquence, le Client autorise la Banque, en adhérant aux présentes conventions, à communiquer les renseignements utiles le concernant à toute personne physique ou morale, intervenant dans le traitement de ses opérations ou l'exécution de ses ordres, et/ou pouvant contribuer à la réalisation des prestations prévues par les présentes conventions ou qui pourraient ultérieurement y être rattachées, notamment aux prestataires de services auxquels la Banque fait ou pourrait faire appel pour l'exécution de travaux sous-traités, et/ou sociétés du groupe pour leur utilisation aux fins d'étude et de gestion des dossiers, de prospections commerciales et/ou d'autres études statistiques. Bien entendu, toutes les mesures sont prises pour assurer la confidentialité des informations transmises.

De plus, il est notamment fait obligation à la Banque, en raison des dispositions pénales sanctionnant le blanchiment de capitaux pouvant provenir d'un trafic de stupéfiants, d'activités criminelles organisées ou de fraude fiscale, de déclarer à TRACFIN les sommes ou opérations dont elle sait ou soupçonne qu'elles proviennent :

- ▶ D'une infraction passible d'une peine privative de liberté supérieure à un an (abus de bien social, escroquerie, abus de confiance, abus de marché etc) ou participant au financement du terrorisme,
- ▶ D'une fraude fiscale,
- ▶ Les opérations dont l'identité du donneur d'ordre, du bénéficiaire, du constituant du fonds fiduciaire ou de tout autre instrument de gestion d'un patrimoine d'affectation reste douteuse malgré toutes les diligences effectuées au titre des vérifications d'identité qui s'imposent à la Banque.

ARTICLE 13 – INTEGRALITE DES ACCORDS ET MODIFICATIONS DU CONTRAT

Le présent contrat, la demande d'abonnement et/ou ses annexes constituent le parfait accord des Parties et se substituent aux conventions antérieures ayant le même objet.

La Banque pourra modifier le présent contrat en informant préalablement le Client par écrit ou sur support durable, par mise à disposition sur le site de la version modifiée du contrat, ce dont il sera informé par courrier ou courrier électronique un mois avant l'entrée en vigueur de ces modifications. L'absence de contestation par le Client avant cette date d'entrée en vigueur vaut acceptation de cette modification.

ARTICLE 14 – DUREE ET RESILIATION

Le contrat est conclu pour une durée indéterminée. Il prend effet à sa date de signature.

Il pourra être mis fin au présent contrat par l'une ou l'autre des Parties, à tout moment, par lettre recommandée avec avis de réception, moyennant le respect d'un préavis de 1 (un) mois à compter de la date de première présentation de ladite lettre.

En outre, le présent contrat pourra être résilié sans délai par l'une ou l'autre des Parties en cas de :

- ▶ Manquement par l'une des Parties à l'une quelconque des obligations lui incombant aux termes des présentes, non réparé dans le délai de dix (10) jours ouvrés à compter de l'envoi, par l'autre Partie, de la lettre recommandée avec avis de réception notifiant le manquement,
- ▶ Liquidation judiciaire de l'autre partie sauf maintien de l'activité tel que prévu à l'article L.641-10 du Code de Commerce
- ▶ Clôture des comptes.

Paraphe
du Client

En cas de cessation du contrat, pour quelque motif que ce soit, les Parties sont tenues de prendre toutes dispositions utiles en vue du dénouement des opérations en cours.

En cas de résiliation du présent contrat, le Client ne pourra plus consulter en ligne les documents mis à disposition dans le cadre du menu e-documents. Il lui appartiendra en conséquence de veiller à les sauvegarder avant la date effective de résiliation.

ARTICLE 15 – EVOLUTIONS DES STANDARDS

Du fait du caractère évolutif des standards utilisés et des systèmes informatiques sur lesquels s'appuient ces standards et des extensions possibles des services convenus, la Banque se réserve la possibilité de renforcer les systèmes de sécurité d'accès, les moyens d'authentification et les systèmes de sécurité d'accès et de dialogue. Elle s'engage, dès qu'elle en aura connaissance, à informer le Client de l'évolution des différents standards et de ses implications potentielles sur les outils logiciels associés à la mise en œuvre de ce dernier.

A partir du moment où la Banque confirme au Client la mise en œuvre effective de l'évolution des standards, le Client et la Banque disposeront d'un délai maximum de douze (12) mois pour en adapter les nouvelles caractéristiques.

Passé ce délai et en cas de désaccord, les parties auront la possibilité de résilier le contrat en respectant les règles définies à l'article 14.

Dans le cas d'évolutions techniques concernant notamment les moyens de sécurité, chaque contractant supportera, pour sa part, les frais de mise à niveau des moyens techniques.

ARTICLE 16 – CESSION

Aucune des parties ne pourra transférer ou céder ses droits, avantages et obligations au titre du contrat sans le consentement préalable écrit de l'autre partie. Nonobstant ce qui précède, le Client autorise la Banque à procéder, sans son consentement préalable écrit, à la cession de tous droits dont elle pourrait bénéficier et à transférer toutes obligations lui incombant à l'une quelconque de ses sociétés affiliées.

ARTICLE 17 – INFORMATIQUE ET LIBERTES

La Banque, en qualité de responsable de traitement, recueille et traite vos données à caractère personnel dans le cadre du présent contrat. Les traitements ont pour finalité la conclusion et l'exécution du présent contrat, ainsi que de permettre à la Banque de vous conseiller, d'évaluer, détecter et gérer le risque client aux fins de remplir son obligation de vigilance. Plus précisément, ces finalités recouvrent la connaissance du client, la gestion du compte et de la relation bancaire et financière, la gestion des produits et services fournis, l'évaluation de l'adéquation et du caractère approprié du service d'investissement fourni, l'octroi de crédit, la fourniture de conseils, notamment dans le cadre de la vente de produits d'assurance, la souscription à distance, par téléphone ou par internet, de produits et services, l'élaboration de statistiques et d'analyse de performances, l'évaluation et la gestion du risque, la prévention des impayés et de la fraude, le recouvrement, la lutte contre le blanchiment de capitaux et le financement du terrorisme et toute obligation légale et réglementaire y compris toute incidence liée à la fiscalité américaine.

La Banque est également amenée à utiliser des moyens d'identification et/ou de géolocalisation de votre adresse IP (Internet Protocol) lorsque vous utilisez la banque en ligne aux fins d'assurer la sécurité et d'être en mesure de détecter des fraudes.

La Banque pourra également traiter des informations concernant la fréquence d'accès, la personnalisation des pages, les opérations réalisées et les informations consultées, ces informations étant inhérentes au fonctionnement du Service.

La base juridique de ces traitements repose sur la relation contractuelle avec la Banque et/ou sur les obligations légales ou réglementaires de la Banque.

Les données à caractère personnel recueillies par la Banque dans le cadre des présentes sont obligatoires pour la conclusion et l'exécution du présent contrat.

La non-fourniture de ces données peut avoir pour conséquence l'impossibilité de conclure ou exécuter le présent contrat.

Vos données à caractère personnel pourront aussi être utilisées pour la réalisation d'animations commerciales, de campagnes publicitaires des sociétés du groupe, enquêtes de satisfaction, ou d'envoi d'information financière. La base juridique de ces traitements repose sur l'intérêt légitime de la Banque, et vous pouvez à tout moment refuser de recevoir de telles offres.

Les données à caractère personnel collectées par la Banque lui permettent également de personnaliser et d'améliorer continuellement la relation commerciale avec ses clients afin de leur proposer des offres les plus adaptées et pertinentes. La Banque pourra être amenée à agréger ces données à caractère personnel afin d'établir des rapports marketings.

La personnalisation des offres de produits et services sur la base d'un profilage fera l'objet en tant que de besoin du recueil de votre consentement, que vous pouvez retirer à tout moment.

Vous êtes informé que la Banque peut être amenée à enregistrer les conversations téléphoniques pour certains types d'opérations, dans le cadre de ses obligations légales ou dans son intérêt légitime. Vos données à caractère personnel seront conservées pour une durée adaptée à la finalité de chaque traitement, sans que cette durée puisse excéder un délai de cinq années après la cessation de la relation contractuelle. Par exception, ces données pourront être conservées pendant des durées plus longues pour gérer les réclamations et contentieux en cours ainsi que pour répondre à nos obligations légales et/ou réglementaires et/ou encore pour répondre aux demandes des autorités autorisées.

Les données à caractère personnel peuvent être transmises à des prestataires de services pour l'exécution des travaux sous-traités et/ou aux sociétés du groupe, et peuvent, à l'occasion de diverses opérations, faire l'objet d'un transfert soit vers un pays de l'Union européenne, soit hors de l'Union européenne.

Les informations relatives aux opérations et aux données personnelles des clients sont couvertes par le secret professionnel auquel la Banque est soumise. Toutefois, elles peuvent être communiquées, à leur requête, aux organismes officiels et aux autorités administratives ou judiciaires habilités à y accéder, notamment dans le cadre de la lutte contre le blanchiment des capitaux ou de la lutte contre le financement du terrorisme.

En vertu du Règlement n° 2015/847 du 20 mai 2015, en cas de transfert de fonds, certaines données à caractère personnel doivent être transmises à la banque du bénéficiaire du virement, située dans un pays de l'Union européenne ou hors Union européenne.

Dans le cas d'un transfert vers un pays hors Union européenne, la sécurité des données à caractère personnel est assurée par la conclusion de clauses contractuelles ou, au sein du groupe ABN AMRO, par des règles contraignantes d'entreprise (BCR). Des règles assurant la protection et la sécurité de ces informations ont été mises en place, en particulier dans le cadre de virements internationaux transitant par SWIFT, consultables sur le site www.fbf.fr.

Tout transfert de données à caractère personnel vers un pays hors Union Européenne ou ne présentant pas un niveau de sécurité adéquat est effectué dans des conditions et sous des garanties propres à assurer la confidentialité et la sécurité de ces données. A ce titre la Banque met en œuvre toutes les mesures techniques et organisationnelles appropriées pour assurer la sécurité de vos données à caractère personnel dans le cadre du transfert.

Les catégories de destinataires concernés pourront vous être communiquées sur simple demande.

Vous disposez du droit de demander l'accès à vos données à caractère personnel et la rectification des données inexacts. Vous pouvez demander l'effacement des données et la limitation du traitement, dans les limites prévues par la législation applicable, étant précisé que l'exercice de ces droits peut, le cas échéant, avoir pour conséquence l'impossibilité de continuer la relation contractuelle avec la Banque. Vous disposez du droit à la portabilité des données à caractère personnel que vous

avez fournies à la Banque, dans les conditions prévues par la législation applicable.

Vous pouvez vous opposer à tout moment à recevoir des communications commerciales.

Vous disposez également du droit de définir des directives générales et particulières relatives à la conservation, à l'effacement et à la communication après votre décès de vos données à caractère personnel traitées par la Banque, conformément aux dispositions législatives et réglementaires applicables. Vos éventuelles directives particulières seront enregistrées par la Banque, et vous pouvez les modifier ou les révoquer à tout moment.

Un Délégué à la protection des données a été nommé pour l'ensemble des entités juridiques du Groupe ABN AMRO. Il exerce ses fonctions au siège social d'ABN AMRO à Amsterdam aux Pays-Bas. Ce Délégué à la protection des données s'est entouré d'une équipe internationale de correspondants locaux à la protection des données.

Vous pouvez exercer les droits dont vous disposez auprès du correspondant français en écrivant à l'adresse électronique suivante NOBC.INFORMATIONDROITDACCES@fr.abnamro.com ou par courrier postal à l'adresse suivante : Banque Neuflyze OBC, Correspondant à la protection des données, 3 avenue Hoche, 75008 Paris, sous réserve de dûment justifier de votre identité en joignant à votre demande une copie d'un titre officiel d'identité.

Si toutefois vous souhaitez vous adresser directement au Délégué à la protection des données du Groupe ABN AMRO, vous pouvez lui écrire par courriel à l'adresse privacy.office@nl.abnamro.com ou par courrier postal à l'adresse suivante : ABN AMRO, Privacy Office, Gustav Mahlerlaan 10, PO Box 283, (PAC : HQ1161), 1000 EA Amsterdam, Pays-Bas.

Vous pouvez introduire une réclamation relative aux traitements de vos données à caractère personnel auprès de la Commission Nationale Informatique et Libertés (CNIL) – www.cnil.fr – 3 place de Fontenoy 75007 Paris.

Vous êtes informé que tout justificatif ou document remis à la Banque pourra être numérisé.

ARTICLE 18 – CONVENTION DE PREUVE

Le Client a la possibilité de signer électroniquement le présent Contrat en recourant à la plate-forme de

signature SIGNHOST (EVIDOS) mise en œuvre par la Banque. L'Utilisateur habilité à signer pour le Client reçoit un courrier électronique comprenant un lien hypertexte qui permet à l'utilisateur d'accéder à la plateforme de signature électronique SIGNHOST. L'Utilisateur doit alors consulter le Contrat, et pour le signer il saisit un code à usage unique qui lui a été envoyé par SMS sur son téléphone mobile. Une fois que le Contrat a été signé par toutes les parties, une copie du Contrat signé électroniquement est envoyée par courrier électronique à l'Utilisateur habilité.

Le Client fait seul son affaire des pouvoirs de signature conférés à l'Utilisateur habilité. Le Client garantit que l'adresse de courrier électronique de l'Utilisateur et son numéro de téléphone mobile lui sont exclusivement réservés. Le Client ne pourra en aucun cas répudier la signature du Contrat dès lors que celle-ci aura été réalisée en utilisant l'adresse de courrier électronique et le numéro de téléphone mobile de l'Utilisateur fournis à la Banque.

Le Client reconnaît la valeur juridique et la force probante de tous documents établis, signés et reçus par l'intermédiaire de la plate-forme de signature SIGNHOST.

Les Parties s'engagent à accepter qu'en cas de litige :

- ▶ Les éléments d'identification, les fichiers de preuve, et les signatures électroniques soient admissibles devant les tribunaux et fassent preuve des données, des consentements et des faits qu'ils contiennent ainsi que des signatures qu'ils expriment ;
- ▶ Les marques de temps soient admissibles devant les tribunaux et fassent preuve des données et des faits qu'elles contiennent.

La plateforme SIGNHOST permet d'assurer la valeur probante et la signature électronique des documents conformément aux articles 1366 et 1367 du Code civil. Le Client reconnaît et accepte que tout document électronique signé électroniquement via la plateforme SIGNHOST a la même valeur probante qu'un document papier et que sa signature électronique l'engage au même titre que sa signature manuscrite.

ARTICLE 19 – DROIT APPLICABLE - JURIDICTION

Le présent contrat est soumis au droit français. En cas de contestation relative à la conclusion, l'interprétation ou l'application du présent contrat, et à défaut de règlement amiable, le Tribunal de Commerce de Paris sera le seul compétent.

Paraphe
du Client