CAISSE D'EPARGNE
ILE-DE-FRANCE

CE net - Conditions générales

en vigueur à compter du 03 décembre 2025

SOMMAIRE

PRÉAMBULE 2

DÉFINITIONS 2

ARTICLE 1 - OBJET 4

ARTICLE 2 - PRINCIPAUX SERVICES DISPONIBLES DANS CE NET 4

ARTICLE 3 - PERSONNES HABILITÉES À UTILISER LE SERVICE 13

ARTICLE 4 - MOYENS MATÉRIELS ET TECHNIQUES D'ACCÈS À CE NET 15

ARTICLE 5 - CONDITIONS D'ACCÈS ET DE SÉCURITÉ DE CE NET 15

ARTICLE 6 - OPPOSITION À L'UTILISATION DES SERVICES EN LIGNE CE NET 20

ARTICLE 7 - CONDITIONS D'EXÉCUTION DES OPÉRATIONS ET ORDRES DE PAIEMENT DÉPOSÉS VIA CE NET, TRANSMIS VIA UN TIERS INITIATEUR DE PAIEMENT (API), OU TRANSMIS VIA UN PROTOCOLE DE COMMUNICATION BANCAIRES EDI 21

ARTICLE 8 - MODALITÉS D'AUTORISATION DES ORDRES DE PAIEMENT 23

ARTICLE 9 - MODALITÉ DE CONFIRMATION DES FICHIERS DE REMISES D'ORDRES DÉPOSÉS VIA LE SERVICE OU TRANSMIS PAR UN PROTOCOLE DE COMMUNICATION BANCAIRE 24

ARTICLE 10 - CONDITIONS D'UTILISATION ET DISPONIBILITÉ DU SERVICE 24

ARTICLE 11 - PREUVE DES OPÉRATIONS ET DÉLAI DE RÉCLAMATION 24

ARTICLE 12 - INTÉGRITÉ, CONFIDENTIALITÉ DU SERVICE 25

ARTICLE 13 - MODIFICATION DES CONDITIONS PARTICULIÈRES ET DES CONDITIONS GÉNÉRALES DE CE NET 25

ARTICLE 14 - TARIFICATION 26

ARTICLE 15 - RESPONSABILITÉS DE LA BANQUE ET DU CLIENT 26

ARTICLE 16 - SECRET PROFESSIONNEL 28

ARTICLE 17 - LUTTE CONTRE LE BLANCHIMENT DES CAPITAUX ET LE FINANCEMENT DU TERRORISME - RESPECT DES SANCTIONS INTERNATIONALES 29

ARTICLE 18 - LUTTE CONTRE LA CORRUPTION ET LE TRAFIC D'INFLUENCE 30

ARTICLE 19 - PROTECTION DES DONNÉES PERSONNELLES 31

ARTICLE 20 - DURÉE ET RÉSILIATION 31

ARTICLE 21 - RÉCLAMATIONS - MÉDIATION 31

ARTICLE 22 - DROIT ET LANGUE APPLICABLES 32

ARTICLE 23 - DOCUMENTS CONTRACTUELS 32

Mod. 07.00.000765 - 11/2025 - DJ CONSEIL : 11/2025 - Page 1/32

PRÉAMBULE

Le présent contrat relatif au Service de Banque à distance CE net (ci-après le « Contrat ») se compose des Conditions Particulières, des présentes Conditions Générales, des Conditions Tarifaires ainsi que de ses éventuelles annexes et avenants. Le Contrat est complété par la convention de compte courant et toutes autres conventions existantes liées à des services spécifiques signées par le Client, par acte séparé, ainsi que le cas échéant par les conventions/contrats liés aux différents protocoles utilisés par le Client (EBICS, SWIFTNET).

Les opérations effectuées dans le cadre du Service ne sauraient déroger aux Conditions Particulières et/ou Générales d'autres produits ou services ouverts ou à ouvrir, sauf stipulation contraire.

DÉFINITIONS

Abonné ou Client : personne physique agissant à des fins professionnelles, ou personne morale ayant souscrit ou utilisant le Service CE net et titulaire d'un compte courant dans les livres de la Banque.

Administrateur(s) : la ou ou les personnes physiques, désignée(s) aux Conditions Particulières du Contrat par le Client, qui a (ont) en charge la gestion des droits des Utilisateurs dans la limite du périmètre de l'abonnement (comptes, Services, Utilisateurs) indiqué aux Conditions Particulières.

Application mobile : Programme téléchargeable de façon gratuite et exécutable à partir du système d'exploitation d'un smartphone ou d'une tablette, permettant aux Personnes habilitées d'utiliser le Service, dans la limite du périmètre strict de leurs habilitations.

Authentification : Procédure qui permet de vérifier l'identité d'une Personne habilitée ou la validité de l'utilisation de l'Instrument de paiement, y compris l'utilisation des données de sécurité personnalisées de cette personne.

Authentification forte : procédure d'Authentification reposant sur l'utilisation d'au moins deux éléments parmi les trois catégories suivantes : 1) une information que la Personne habilitée est seule à connaître (mot de passe, code secret, code PIN), 2) l'utilisation d'un appareil qui appartient à la Personne habilitée (téléphone portable, montre connectée, appareil dédié fourni par la Banque...), 3) une caractéristique personnelle qui est intimement liée à la Personne habilitée (empreinte digitale, reconnaissance faciale, vocale...).

Espace de Banque à distance : espace sécurisé propre au Client, accessible par internet depuis le Site ou depuis l'Application mobile de la Banque où le Service est disponible.

Banque : désigne la Caisse d'Epargne fournissant le Service.

CE net : désigne le service de Banque à distance fourni par la Banque à des fins d'utilisation professionnelle.

Certificat électronique : Document électronique attestant du lien entre les données de vérification de Signature électronique et un signataire.

CFONB : Comité Français d'Organisation et de Normalisation Bancaires.

Compte donneur d'ordre : compte à partir duquel l'opération est initiée par le donneur d'ordre.

Collège de signature : Regroupement d'Utilisateurs détenant une délégation de signature des remises d'ordre pour valider un même périmètre d'opérations définies aux Conditions Particulières. Le Service permet de paramétrer les droits de signature de l'abonnement CE net au niveau d'un groupe d'Utilisateurs signataires qui forment alors un Collège de signature.

Compte destinataire : compte vers lequel l'opération est initiée par le donneur d'ordre.

Digital Box : Ce service permet au Client de bénéficier de la mise à disposition, en format électronique, de certains documents lis à la gestion d'un produit bancaire. Les conditions générales d'utilisation de Digital Box complètent les présentes conditions générales.

Digital Share : Service d'échange de documents entre le Client et la Banque.

Données de sécurité personnalisées : données confidentielles fournies par la Banque à un Client ou un Abonné pour l'utilisation d'un Instrument de paiement. Ces données, propres au Client et placées sous sa garde, visent à l'authentifier et à sécuriser ses opérations dans le cadre de CE net.

EDI : Echanges de Données Informatisées ou Electronic Data Interchange peut être défini comme l'échange, d'ordinateur à ordinateur, d'entreprises à établissements bancaires, de données concernant des transactions en utilisant des réseaux de

télécommunication et des formats normalisés, directement exploitables par leurs systèmes d'informations. L'EDI peut se faire selon différents protocoles, dont notamment le protocole EBICS. Pour bénéficier du service EDI, le Client doit conclure avec la Banque le contrat relatif à l'EDI et/ou le contrat relatif au protocole d'échange retenu, tel le protocole EBICS.

EBICS : Electronic Banking Internet Communication Standard. Protocole multi-bancaire utilisé sur Internet avec un haut niveau de sécurité permettant une Authentification réciproque par Certificats. Deux modes d'utilisation d'EBICS se distinguent dans le sens Client vers Banque : EBICS profil T (transport) et EBICS profil TS (Transport et Signature). Le Client doit s'équiper d'un logiciel de communication EBICS T ou EBICS TS pour pouvoir utiliser le protocole EBICS. EBICS permet des échanges de fichiers volumineux.

EBICS profil T : Les fichiers envoyés par le Client à la Banque ne sont pas accompagnés de la ou des signature(s) personnelle(s) jointe(s). Les données envoyées ne pourront être prises en compte que si la Banque se trouve en possession d'un ordre de validation transmis par un autre canal.

EBICS profil TS : Les fichiers envoyés par le Client à la Banque sont accompagnés dans la même transmission de la ou des signature(s) personnelle(s) jointe(s) prévue(s) pour l'échange des données concernées.

Instrument de paiement : dispositif personnalisé et/ou un ensemble de procédures convenu entre le Client et la Banque utilisé(s) pour donner un ordre de paiement.

Jour Ouvrable : désigne un jour au cours duquel la Banque ou la banque du bénéficiaire ainsi que tous les autres intervenants à l'exécution d'une opération de paiement exercent une activité permettant d'exécuter celle-ci.

Lecteur CAP : appareil lecteur de carte à puce fourni par la Banque à l'Utilisateur du service SOL par lecteur CAP (Sécurisation des Opérations en Ligne). Il nécessite l'utilisation d'une carte business ou d'une carte Secur@ccès afin de fournir un code de contrôle.

Messagerie Sécurisée Internet (MSI) : Dans le cadre de l'abonnement à CE net, le Client et les Utilisateurs ont accès à une messagerie électronique dans l'environnement sécurisé de CE net, dénommée la « Messagerie Sécurisée Internet » (ci-après « MSI »), dont les Conditions Générales d'Utilisation figurent à l'article 2.1.2.6 ci-après.

Opérations sensibles : opérations de Banque à distance nécessitant une Authentification forte afin de prévenir le risque de fraude.

Personnes habilitées : désigne l'Utilisateur Principal, les Administrateurs et les Utilisateurs autorisés à agir au nom et pour le compte du Client.

Parafeur : Espace dédié à la Signature électronique des remises d'ordres.

Pare-feu (firewall) : Dispositif qui protège un système informatique connecté à Internet des tentatives d'intrusion.

Référentiel : ensemble des Comptes destinataires de l'abonnement CE net du Client.

Relevés d'opérations : relevés détaillés des opérations reçues, rejets sur des opérations émises.

Services : Ensemble des fonctionnalités de CE net.

Services CE net « aller » : Echanges de Données Informatisées du Client vers la Banque.

Services CE net « retour » : Echanges de Données Informatisées de la Banque vers le Client.

Site : désigne le site Internet permettant l'accès aux Services de CE net.

Signature électronique : Signature utilisant un procédé électronique fiable d'Identification de son auteur et garantissant son lien avec l'acte auquel elle s'attache.

Synthèse des comptes : La Synthèse des comptes permet au Client d'avoir une vision globale du solde de chacun de ses comptes.

Transporteur de données : « Utilisateur » technique qui transfère et réceptionne les flux via un logiciel de communication bancaire. Il ne peut pas avoir de droit de signature bancaire sur les flux. Il est compatible avec les protocoles EBICS, Swift Net (FileAct et FIN).

TurboSign : Extension du navigateur internet qui permet de faire dialoguer CE net depuis un navigateur Chrome ou Firefox avec le Certificat électronique. L'installation de cette extension est proposée à l'utilisateur à la première utilisation du Certificat dans CE net. Cette extension est à installer sur chaque poste de travail sur lequel le Certificat électronique sera utilisé.

Utilisateur Principal : personne physique, désignée aux Conditions Particulières du Contrat qui peut utiliser le Service, dans l'ensemble du périmètre de l'abonnement indiqué aux Conditions Particulières, et qui a également le profil d'Administrateur dans les limites des fonctions accessibles en ligne.

Utilisateur(s) : la ou les personnes, désignée(s) aux Conditions Particulières du présent contrat, habilitée(s) à utiliser le Service, dans le périmètre qui lui (leur) a été imparti par le ou les Administrateurs et le cas échéant par l'Utilisateur Principal, et dans les limites des fonctions accessibles en ligne.

ARTICLE 1 - OBJET

Le Contrat détermine les conditions d'accès et d'utilisation du Service de Banque à Distance CE net fourni par la Banque. Ce Service permet au Client par l'intermédiaire des Personnes habilitées, d'effectuer des opérations à distance selon les options retenues :

- la consultation de son ou ses comptes, l'obtention de divers renseignements liés à différents produits qu'il détient, la réalisation d'opérations portant sur son ou ses comptes (saisie d'ordres de paiement, gestion et suivi des ordres en ligne, ...), la possibilité de souscrire à des contrats et services complémentaires (sous réserve d'être préalablement habilité à souscrire le contrat ou service et à engager le Client).
- les Echanges de Données Informatisées (EDI), la saisie d'opérations, la gestion et le suivi des ordres en ligne, ainsi qu'un service de Signature électronique. Pour ce faire, la Banque met à la disposition du Client :
  - des protocoles de communication bancaire tels que EBICS, SWIFTNet, FileAct ou SWIFTNet FIN permettant l'EDI dans les deux sens de la relation (Client/banque : émission d'ordres & banque/Client : réception de relevés...) et des services associés sur le serveur EDI de la Banque,
  - un Site sécurisé permettant le dépôt de remises d'ordres, la récupération de relevés et des services associés.

Le Service est disponible depuis l'Espace de Banque à distance du Client. Certains services/fonctionnalités sont disponibles uniquement via le Site ou via l'Application mobile.

Le Client souscrit à tout ou partie du Service dans les Conditions Particulières du Contrat.

Le Client s'engage à remettre à l'ensemble des Personnes habilitées à utiliser CE net, un exemplaire des présentes Conditions Générales ainsi que les conditions générales de la convention de compte courant, et de toutes leurs modifications à venir.

La Banque se réserve le droit de modifier le contenu du Service et/ou de l'une ou de l'ensemble des fonctionnalités du Service notamment en vue d'en améliorer la qualité ou par l'adjonction de nouvelles fonctionnalités. Le cas échéant, le Client sera informé des éventuels impacts contractuels et tarifaires dans les conditions prévues à l'article 13 du Contrat.

ARTICLE 2 - PRINCIPAUX SERVICES DISPONIBLES DANS CE NET

Le Client désigne aux Conditions Particulières du Contrat lors de la souscription la liste des comptes concernés par l'abonnement, les services auxquels il souhaite souscrire, les types d'opération et, le cas échéant, les formats de fichiers associés, ainsi que les Personnes habilitées à utiliser le Service.

Toute modification de ces choix donnera lieu à la signature d'avenants aux Conditions Particulières sauf, sous réserve de disponibilité, si cette modification résulte d'un choix du Client effectué directement par ce dernier sur son Espace de Banque à Distance.

CE net se décline en 3 offres en fonction des besoins du Client : CE net Comptes, CE net Remises et CE net EDI. Une offre spécifique CE net COPRO peut également être proposée par la Banque.

2.1 - CE net Comptes

CE net Comptes permet au Client d'effectuer par l'intermédiaire des Personnes habilitées à utiliser le Service, les principales opérations décrites ci-après (la liste n'étant pas exhaustive).

2.1.1 - Gestion des accès à CE net Comptes

L'accès des Utilisateurs à CE net Comptes est paramétré à la fois lors de la souscription par le Client dans les Conditions Particulières mais aussi via son Espace de Banque à distance à partir de l'onglet « Paramétrage », en cliquant sur « Gestion des utilisateurs ».

2.1.2 - Principaux Services disponibles dans CE net Comptes

2.1.2.1 - Consultation

- <u>CONSULTATION DES COMPTES ET DES OPÉRATIONS</u>
  Le Client peut consulter la position du ou de ses comptes (en date comptable ou en date de valeur), compris dans le périmètre du Service, les dernières opérations de débit et/ou de crédit intervenues sur le ou les comptes, sous réserve qu'elles

ne remontent pas à plus de cent quatre-vingts jours (180) jours, ainsi que les débits en instance de la/des carte(s) bancaire(s) s'il y a lieu.

Le Client peut consulter les opérations à venir, ainsi que le solde prévisionnel de son ou de ses comptes courant(s) sur les sept (7) jours à venir. Ces informations sont communiquées à titre indicatif, seules les écritures mentionnées sur le relevé de compte ou l'arrêté de compte faisant foi entre les parties.

Il est possible de télécharger le détail des opérations.

- CONSULTATION DE L'ACTIVITE MONÉTIQUE
  Le Client peut consulter certains de ses contrats monétiques, ainsi que ses locations de matériel (terminal de paiement électronique) souscrits auprès de la Banque. Il peut également consulter via un tableau de bord, l'ensemble de son activité monétique.

- CONSULTATION ET GESTION DES MANDATS DE PRÉLÈVEMENT SEPA ET DES OPÉRATIONS DE PRÉLÈVEMENTS REÇUS AU DÉBIT DU COMPTE
  Le Client a la possibilité de consulter les mandats de prélèvements SEPA CORE, les prélèvements exécutés et à venir, de bloquer et réactiver les prélèvements et de gérer les mandats de prélèvements SEPA interentreprises reçus en attente d'être débités sur son compte ou déjà débités.

- CONSULTATION ET GESTION DES OPÉRATIONS SUR TITRES ET VALEURS MOBILIÈRES
  CE net Comptes permet au Client, sur option, la passation d'opérations sur titres financiers sous réserve de la signature préalable d'une convention de compte d'instruments financiers.

- GAMME DE SERVICES TRESEO
  Sous réserve de disponibilité, cette gamme de services permet d'accéder au(x) service(s) TRESEO souscrit(s) par le Client pour visualiser l'ensemble des informations dédiées à ces offres, accéder aux reportings et aux documents produits.

2.1.2.2 - Opérations sur les comptes

- VIREMENTS
  Les Personnes habilitées pourront enregistrer des Comptes destinataires et créer des listes de destinataires selon leurs profils. Les Personnes habilitées pourront effectuer des virements unitaires de compte à compte ouverts dans les livres de la Banque au sein du périmètre des Comptes donneur d'ordre indiqué dans les Conditions Particulières, effectuer des virements SEPA, de manière unitaire ou groupée (sous réserve de disponibilité), vers des Comptes destinataires préalablement enregistrés dans le Référentiel de l'abonnement. Dès la validation du ou des virements, via une authentification forte, les ordres sont enregistrés. Les ordres de virements à exécution immédiate sont irrévocables dès leur réception par la Banque.

  Le Client a la possibilité de révoquer un ordre de virement permanent ou à exécution différée dans les conditions indiquées dans la partie relative aux « Services de paiement » de sa convention de compte courant.

  Les ordres de paiement et les opérations qui en découlent sont soumis aux conditions de traitement habituelles en vigueur dans la Banque, à la date de l'opération et objet de la convention de compte courant régularisée par acte séparé par le Client, sauf conditions spécifiques prévues dans les conditions particulières de la convention de compte courant, et/ou dans les Conditions Particulières du Contrat.

  Le Client peut suivre les opérations transmises dans le suivi des ordres.

  Le montant maximum de virement accepté par la Banque est indiqué au Client par le Service ou, le cas échéant, aux Conditions Particulières ou encore dans tout autre document destiné au Client. Ces montants limites peuvent aussi être fournis par la Banque, à la demande du Client.

  Pour garantir le bon déroulement de ses virements, il est recommandé au Client de contrôler ses bénéficiaires existants ou lors de l'ajout d'un bénéficiaire sur sa liste, en s'assurant que les noms des bénéficiaires correspondent exactement aux noms enregistrés sur leurs comptes bancaires :
  - Le nom et le prénom lorsque le bénéficiaire est une personne physique ;
  - La raison sociale ou le nom commercial lorsque le bénéficiaire est une personne morale (entreprises, associations, ...).

  Ces informations sont disponibles sur le Relevé d'identité bancaire (RIB) du bénéficiaire. Il convient de ne pas utiliser des abréviations ou des surnoms. Toute différence, même minime, ou toute autre information que le prénom et le nom ou la raison sociale ou le nom commercial, pourrait entraîner une non-concordance dans le cadre du service de vérification du bénéficiaire décrit ci-après.

  La mise à jour de la liste des bénéficiaires relève de la propre initiative du Client. La Banque ne contactera jamais le Client (par téléphone ou par un autre moyen) pour lui proposer de l'accompagner dans cette démarche.

<u>Vérification du bénéficiaire - Virements SEPA classiques et instantanés</u> (service permettant de renforcer la sécurité des virements et de réduire les risques d'erreurs et de fraudes)

- Principes généraux

Conformément au Règlement (UE) 2024/886 du 13 mars 2024, la Banque, en tant que banque du payeur, procède à la vérification du bénéficiaire auquel le Client a l'intention d'envoyer un virement SEPA classique ou instantané. Ce service vérifie la concordance entre l'IBAN du compte du bénéficiaire et le nom de ce dernier. Etant précisé que le nom du bénéficiaire correspond au nom et prénom, dans le cas d'une personne physique, au nom commercial ou à la dénomination sociale ou à un autre élément de données accepté par la Banque, dans le cas d'une personne morale.

Cette vérification est réalisée dès que le Client a complété les informations relatives au bénéficiaire, dans l'ordre de virement, et avant qu'il autorise le virement dans son Espace de banque à distance, accessible via le site internet ou l'application mobile de la Banque.

Pour les virements différés et permanents, la vérification est effectuée lors de la constitution de l'ordre de virement par le Client et non à chaque échéance du virement.

Aucune vérification n'est effectuée lorsque le Client ajoute le compte d'un bénéficiaire dans sa liste de bénéficiaires de virements.

Ce service est fourni au Client à titre gratuit.

- Résultats de la vérification

A la demande de la Banque, cette vérification est effectuée par le prestataire de services de paiement du bénéficiaire qui transmet sa réponse à la Banque.

En cas de concordance, le parcours de virement se poursuit.

Dans les autres cas, le résultat de la vérification des bénéficiaires est mis à disposition du Client par la Banque, avant la validation de l'ordre saisi. Ce résultat n'est valable qu'au moment de la mise à disposition du rapport par la Banque au Client, et ne saurait en aucun cas prévaloir pour l'avenir.

En cas de concordance partielle et de non-concordance, la Banque informe le Client que l'autorisation du virement pourrait conduire à ce que les fonds soient virés sur le compte d'un autre bénéficiaire que celui auquel le Client souhaite transmettre les fonds.

- En cas de concordance partielle, la Banque communique au Client le nom du bénéficiaire associé à l'IBAN qu'il a fourni. Le Client a alors la possibilité :
  - Soit, de corriger le nom du bénéficiaire et d'autoriser le virement. Le nom du bénéficiaire est ainsi automatiquement modifié dans la liste de bénéficiaires de virements du Client.
  - Soit d'autoriser le virement sans modifier le nom du bénéficiaire.
  - Soit d'annuler le virement.

- En cas de non-concordance, le Client en est immédiatement informé. La Banque ne lui donne aucune information sur le bénéficiaire. Le Client a alors la possibilité :
  - Soit, d'annuler le virement et s'il le souhaite de modifier le nom du bénéficiaire dans sa liste de bénéficiaires de virements, et de réémettre un nouveau virement qui sera soumis à une nouvelle vérification du bénéficiaire.
  - Soit, d'autoriser le virement sans corriger le nom du bénéficiaire dans sa liste de bénéficiaires.

Le Client est également informé lorsque la banque du bénéficiaire ne permet pas de vérifier le nom du bénéficiaire associé à l'IBAN. Le Client pourra alors annuler le virement ou l'autoriser.

Si, malgré les alertes, le Client autorise le virement, la Banque l'informe :
- Que le virement est considéré comme exécuté au profit du bon bénéficiaire ;
- Qu'elle ne peut pas être tenue responsable de l'exécution de ce virement au profit d'un mauvais bénéficiaire ;
- Qu'il n'a pas droit au remboursement de ce virement pour opération mal exécutée.

De même, la Banque n'est pas responsable de l'exécution d'un virement SEPA en faveur d'un mauvais bénéficiaire, sur la base d'un IBAN inexact communiqué par le Client, pour autant que la Banque ait satisfait à ses obligations au titre du service de vérification du bénéficiaire.

En cas de non-respect par la Banque ou un prestataire de services d'initiation de paiement de ses obligations en matière de vérification du bénéficiaire, entraînant une opération de paiement mal exécutée, la Banque restitue sans tarder au Client le montant du virement SEPA et, le cas échéant, rétablit le compte dans la situation qui aurait prévalu si l'opération n'avait pas eu lieu.

Si le compte du bénéficiaire est clôturé, le Client en est également informé et le virement ne peut pas être exécuté.

- Description du service lorsque la Banque agit en tant que banque du bénéficiaire
A la demande de la banque du payeur, la Banque est tenue de vérifier la concordance entre l'IBAN du compte et le nom du bénéficiaire, fournis par le payeur. La Banque informe la banque du payeur du résultat de cette vérification. En cas de concordance partielle, la Banque a l'obligation réglementaire de communiquer à la banque du payeur le nom du Client bénéficiaire du virement.

- PAIEMENT D'EFFETS DE COMMERCE
  CE net Comptes permet au Client d'être informé de la présentation des lettres de change et des billets à ordre à honorer et, le cas échéant, de gérer ces derniers conformément aux dispositions prévues dans la convention de compte courant qu'il a signée.

- CONSULTATION DES ENCOURS DAILLY
  CE net permet au Client, la consultation détaillée des encours de créances Dailly (par Avance ou en Garantie), sur les comptes cédants compris dans le périmètre de son abonnement. La faculté de consultation de la part du Client ne présume pas de l'octroi d'une ligne de cession de créances professionnelles (DAILLY).

- CESSION DÉMATÉRIALISSÉE DE CRÉANCES PROFESSIONNELLES
  Sous réserve que le Client dispose d'une ligne de cession de créances professionnelles octroyée par la Banque, CE net permet au Client et aux Utilisateurs de céder des créances dématérialisées (par Avance ou en Garantie), sur les comptes cédants compris dans le périmètre de son abonnement, en permettant notamment le dépôt et la signature de ses bordereaux de cession dématérialisés (Service e-Dailly).

2.1.2.3 - Opérations de financement
CE Net compte permet la consultation des contrats de crédits court, moyen, long terme ainsi que des engagements par signature. Outre la consultation des crédits octroyés au Client, les personnes dûment habilitées à représenter le Client pourront signer électroniquement une opération en lien avec ses crédits.

2.1.2.4 - Contrat d'assurance
Le Client peut visualiser les références des contrats d'assurance souscrits auprès de la Banque.

2.1.2.5 - Moyens de paiement

- PILOTAGE DE LA CARTE BUSINESS ET CONSULTATION DES OPÉRATIONS
  CE Net Comptes permet à un porteur de carte, Utilisateur de CE net, de pouvoir effectuer le pilotage de la carte Business dans les conditions précisées au contrat porteur carte signé avec la Banque.

  Sous réserve de disponibilité, un Administrateur pourra également augmenter temporairement le plafond de la carte d'un des porteurs sous réserve que la carte soit incluse dans le périmètre de l'abonnement.

  La Personne habilitée pourra consulter les opérations réalisées avec sa carte business et/ou les opérations des autres cartes business rattachées à l'abonnement du Client.

- OPPOSITION SUR CHÉQUIERS ET CARTES BANCAIRES
  CE net Comptes permet au Client d'obtenir les informations utiles aux modalités d'opposition pour les chèques et cartes bancaires.
  Le cas échéant, toute opposition devra être complétée, dans les quarante-huit (48) heures, des documents sollicités à adresser à la Banque.

- COMMANDE DE CHÉQUIER
  CE net Comptes permet au Client, à condition d'y avoir été habilité et d'être équipé d'un moyen d'Authentification forte (cf. article 5), de commander en ligne des chéquiers, si celui-ci n'a pas opté pour le renouvellement automatique.

- COMMANDE DE BORDEREAUX DE REMISE DE CHÈQUES
  CE net Comptes permet au Client, à condition d'y avoir été habilité, de commander en ligne des bordereaux de remise de chèques qui seront livrés à l'adresse précisée lors de la souscription du service auprès de la Banque.

2.1.2.6 - Autres services

- DIGITAL SHARE
  Le service d'échange de document permet aux Personnes habilitées de visualiser les demandes de documents de la Banque et suivre leur état d'avancement, et de déposer des documents à destination de la Banque sous format électronique *(notamment pdf, jpeg, ...)*.

La Banque notifie l'Utilisateur Principal et l'Administrateur par message électronique lors de la création d'une demande de document, d'une relance ou lors du rejet d'un document déposé. La Banque est avertie dès qu'un document est déposé par l'Utilisateur Principal ou un Administrateur.

- MESSAGERIE SÉCURISÉE INTERNET OU MSI (CONDITIONS GÉNÉRALES D'UTILISATION)

• Description du service

Dans le cadre de l'abonnement à CE net souscrit par le Client, chaque Utilisateur a accès à une messagerie électronique dédiée dans l'environnement sécurisé de CE net, dénommée la « Messagerie Sécurisée Internet » (ci-après « MSI »). Le Client et les Utilisateurs sont informés que le premier accès à la MSI vaut acceptation des présentes Conditions Générales d'Utilisation dont ils doivent prendre connaissance au préalable. Les messages sont consultables par les Utilisateurs pendant un délai de 90 (quatre-vingt dix) jours à compter de leur réception.

• Accès à la messagerie Sécurisée Internet

La MSI est exclusivement accessible aux Utilisateurs de CE net. Toute utilisation du Service sera réputée avoir été effectuée par un Utilisateur. Le Client est informé qu'en résiliant son abonnement à CE net, il met fin à l'accès à la Messagerie Sécurisée Internet de tous les Utilisateurs. Dans ce cas, le Client et les Utilisateurs perdent définitivement l'accès aux messages conservés jusqu'alors dans leur MSI. Il appartient au Client d'alerter en temps utile l'ensemble des Utilisateurs des conséquences de la résiliation de l'abonnement CE net sur leur MSI.

La suppression d'un Utilisateur de l'abonnement CE net du Client entraine immédiatement la fermeture et la suppression de la MSI de cet Utilisateur. Il appartient au Client de prendre préalablement ses dispositions.

• Fonctionnalités du service

- Interlocuteurs des Utilisateurs :
La MSI permet à l'Utilisateur d'adresser, ou de recevoir, des messages électroniques en direction, ou en provenance, d'une ou plusieurs personnes du réseau des Caisses d'Epargne dont la liste est définie par la Banque.

- Notification d'un nouveau message dans la Messagerie Sécurisée Internet :
Sous réserve de la disponibilité de ce service dans la Banque et de la déclaration préalable d'une adresse électronique personnelle valide à usage professionnel, l'Utilisateur peut recevoir une notification électronique des nouveaux messages parvenus dans sa MSI. La Banque n'est pas responsable de la saisie erronée des données personnelles de l'Utilisateur, du filtrage anti-spam abusif du transport des données, de la qualité et de la disponibilité des réseaux de télécommunication, ni des interruptions pour les interventions de maintenance, par suite de cas fortuits ou de force majeure et, en particulier, celles qui se produisent à la suite d'un mauvais fonctionnement du matériel de l'Utilisateur ou du réseau de télécommunications.
La Banque dégage sa responsabilité des difficultés associées au contrat passé entre le Client et son fournisseur d'accès.
La MSI est un vecteur de communication des notifications que le Client recevra pour l'informer de la mise à disposition des relevés/documents électroniques dans son espace CE net.

- Suppression des messages :
L'Utilisateur a la possibilité de supprimer de la MSI des messages électroniques émis ou reçus par lui. Dans ce cas, aucune restauration de ces messages ainsi supprimés ne sera possible ultérieurement. Par ailleurs, les messages électroniques transmis et reçus resteront disponibles pendant 90 (quatre-vingt-dix) jours, au-delà de ce délai, ils sont purgés.

- Limite à la capacité de stockage :
La MSI attribuée à l'Utilisateur est limitée dans sa capacité de stockage en raison des contraintes techniques et/ou de sécurité retenues par la Banque, susceptibles d'évoluer dans le temps. L'espace de messagerie effectivement utilisé est visible dans la Messagerie sécurisée de l'Utilisateur. En cas de dépassement de cette capacité de stockage, la Banque pourra être amenée à supprimer les messages diffusés en automatique, à caractère commercial ou bien relatifs à la gestion des comptes de l'Utilisateur.

• Contenu des messages

- Règles d'utilisation de la MSI :
La MSI est exclusivement un service de dialogue entre l'Utilisateur et des interlocuteurs de la Banque. L'Utilisateur s'engage à n'utiliser la MSI que dans le cadre strictement limité à la relation bancaire définie par le Service CE net. Aussi, l'Utilisateur s'interdit de transmettre tout message, pièce jointe ou autre document qui n'aurait aucun lien direct, voire indirect avec l'objet de CE net. La MSI n'est pas destinée à la prise en compte des demandes relatives aux opérations bancaires, aux opérations sur instruments financiers et à l'inscription de comptes destinataires de virements. L'Utilisateur est tenu soit d'effectuer ses opérations conformément aux dispositions de CE net, soit de transmettre ses demandes à la Banque qui gère les comptes du Client. L'Utilisateur devra faire un usage raisonnable du service, notamment quant au contenu, à la fréquence des messages envoyés ou à la taille ou au format des pièces jointes, toute autre utilisation pouvant notamment être à l'origine d'une saturation de l'infrastructure informatique de nature à mettre en péril la qualité et la

continuité du service. En cas d'utilisation déraisonnable, la Banque se réserve le droit de mettre en demeure le Client, par tous moyens, de cesser une telle utilisation. A défaut de changement de sa part, la Banque se réserve le droit de résilier le Service, sans que le Client puisse prétendre à une quelconque indemnité, en raison notamment de la perte des messages contenus dans la MSI ainsi supprimée.

- Traitement d'une demande formulée dans un message :
  En l'absence de réponse de l'interlocuteur dans un délai raisonnable, l'Utilisateur est invité à contacter la Banque par tout autre moyen. La prise en compte des demandes de mise à jour des données et des informations personnelles de l'Utilisateur pourra être conditionnée par la Banque à la présentation par le Client des pièces justificatives correspondantes.

• **Sécurité**
L'Utilisateur est tenu de vérifier la qualité des documents électroniques joints à ses messages, en veillant notamment à ce qu'ils ne comportent pas de virus ou autres logiciels malveillants. La Banque se réserve le droit de supprimer les documents électroniques attachés aux messages échangés qui menaceraient directement ou indirectement l'intégrité de son système d'information. La Banque met en œuvre ses meilleurs efforts afin d'assurer la non-dangerosité des messages envoyés à l'Utilisateur via la MSI ; mais elle ne peut, compte tenu des aléas techniques, le garantir complètement. Il appartient, en conséquence, au Client et à l'Utilisateur de mettre en œuvre les mesures adéquates afin de préserver l'intégrité du poste informatique de l'Utilisateur. En tout état de cause, la Banque ne saurait être tenue responsable en cas de dommages causés au poste informatique de l'Utilisateur.

• **Archivage des messages par l'Abonné**
La Banque rappelle au Client ainsi qu'aux Utilisateurs qu'il leur appartient de mettre en œuvre régulièrement les procédures de sauvegarde (copies d'écrans, copie du texte dans un document électronique, export dans un fichier au format PDF, etc.) adéquates afin d'archiver sur le système informatique du Client tous les documents ou messages stockés dans leur MSI, notamment afin de tenir compte de la possibilité pour la Banque de fermer, et de supprimer le cas échéant, l'accès au Service ou encore de supprimer des messages en cas d'atteinte à la capacité de stockage de ladite Messagerie. La Banque ne saurait être tenue pour responsable en cas de perte par le Client des documents et messages susmentionnés qui n'auraient pas été correctement sauvegardés.

• ACCÈS FACILITÉ À CERTAINS SERVICES
CE net Comptes permet aux Utilisateurs ou le cas échéant au représentant légal seul, l'accès sans nouvelle Identification/Authentification à certains services proposés par la Banque (PulCEo Connect ...) et/ou d'autres entités du Groupe BPCE à condition pour le Client d'y avoir souscrit et d'y être habilité.

Le Client reconnait que toute opération réalisée sur l'un de ces services et consécutive à ce dispositif d'accès lui sera opposable et l'engagera à l'égard des entités proposant ces services. Cette opération sera soumise aux conditions générales d'utilisation de ces espaces.

2.1.3 - Services optionnels disponibles dans CE net Comptes

• SUIVI DES OPÉRATIONS SWIFT GPI
Le service SWIFT - GPI permet au Client, sous réserves de souscription et d'habilitations, de consulter l'état d'avancement de certaines de ses opérations internationales.

• SERVICE DIGITAL BOX
Le service « Digital Box » permet au Client et aux Personnes habilitées de télécharger et consulter sous forme électronique via l'abonnement CE net les relevés de compte et tous les documents dématérialisés disponibles. L'activation et la résiliation de ce service sont effectuées par le Client auprès de la Banque.

• SERVICE DE GESTION DE FACTURES

• **Description du service Gestion de factures**
Pour accéder au service de Gestion de factures, sous réserve de disponibilité de ce service, le Client doit être équipé du Service CE net Comptes ou CE net Remises et d'un compte courant professionnel.

Le Client peut souscrire le service de Gestion de factures via son Espace de banque à distance, le cas échéant, avec l'aide de son conseiller.

Seul l'Utilisateur principal peut souscrire et utiliser le service de Gestion de factures sous réserve d'être habilité à souscrire le service et à engager le Client.

Les principales fonctionnalités disponibles dans le service de Gestion de factures sont les suivantes (selon le niveau de service qu'il choisit, le Client peut ne pas disposer de certaines fonctionnalités) :
• Création de devis et édition de factures électroniques pour ses propres clients, avec possibilité d'y insérer un lien de paiement afin d'être réglé par virement : Le Client peut créer des devis, éditer des factures avec ou sans lien de paiement et

bénéficier de services connexes, tels que le suivi des paiements en temps réel et les relances automatiques des impayés. A ce titre, le Client, mandant, confie à la Banque, mandataire, dans le respect des règles économiques et fiscales applicables, l'établissement et l'émission de ses factures. A cet égard, le Client donne expressément mandat à la Banque d'établir en son nom et pour son compte des factures originales afférentes à tout type de prestations de services ou d'achat et ce conformément à la réglementation fiscale et économique en vigueur, et en particulier les dispositions des articles 289, I-2 et 242nonies, I (Annexe 2) du Code général des impôts. Il incombe au Client d'indiquer à la Banque son assujettissement ou non à la TVA et toutes les informations nécessaires à l'établissement de ses factures. Lesdites factures seront à la disposition du Client sur son Espace de banque à distance.

- Import et collecte automatisée des factures fournisseurs et paiement : La Banque procède à la collecte automatique des factures fournisseurs du Client à partir (i) de l'email du Client et/ou (ii) de son espace client sur les sites fournisseurs. La Banque procède alors à l'extraction des informations clés figurant dans les factures. Le Client a la possibilité de payer ses factures via le service de Gestion de factures.
- Le stockage : La Banque propose des espaces de stockage permettant au Client de stocker tout type de document.
- Le rapprochement bancaire assisté et la synchronisation des comptes bancaires externes (voir ci-dessous) : Le Client peut comparer les factures avec les transactions bancaires effectuées depuis le(s) compte(s) courant(s) professionnel(s) détenus auprès de la Banque, mais aussi auprès d'autres banques, sous réserve d'avoir inclus ces autres comptes dans le périmètre de la synchronisation.
- Gestion des notes de frais : la Banque met à la disposition du Client et de ses collaborateurs une application mobile dédiée aux notes de frais permettant de les scanner et de les ajouter dans le service, à télécharger sur les appareils compatibles depuis les espaces de téléchargement d'applications (Google Play, Apple Store, etc…). La Banque procède ensuite à l'extraction et à la saisie automatique des informations relatives aux montants et aux dates desdites notes de frais.
- Suivi du prévisionnel de trésorerie : selon le niveau de service choisi, le Client peut suivre l'évolution de sa trésorerie, ses budgets et objectifs.
- Gestion et export des documents et écritures vers les logiciels comptables et possibilité d'accès externalisé à l'espace gestion de factures pour le comptable du Client : Le Client peut inviter son comptable externe à accéder au service de Gestion de factures en renseignant les coordonnées et l'adresse électronique de ce dernier. Cette invitation est entièrement sous la responsabilité du Client qui peut à tout moment révoquer l'accès accordé. Le comptable dispose d'un accès limité via une interface dédiée, lui permettant d'effectuer des actions spécifiques liées à la préparation de la comptabilité, comme par exemple consulter les opérations/justificatifs comptables et bancaires et les télécharger si besoin. Le comptable ne peut pas créer ou ajouter d'autres accès au sein du service de Gestion de factures, ni accéder à d'autres fonctionnalités de l'Espace de banque à distance du Client. Il n'a pas non plus la possibilité de procéder à des paiements ou à des encaissements, ni d'effectuer d'autres opérations qui pourraient engager l'entreprise.
- « Paiement des factures fournisseurs », « Encaissement via lien de paiement inséré dans les factures clients » et « Synchronisation des comptes bancaires externes », disponibles dans le service de Gestion de factures, s'appuient sur :
  - les services d'information sur les comptes, également appelés agrégation de comptes (intitulés « Synchronisation des comptes bancaires » dans le service de Gestion de factures) et d'initiation de paiement fournis par Perspecteev (Bridge) ;
  - le service d'information sur les comptes fournis par Powens.

  Afin d'accéder à ces services, le Client sera redirigé par un lien URL vers le site internet de ces prestataires et entrera en relation contractuelle directe avec celui-ci conformément à leur Conditions Générales et Politique de confidentialité rendues accessibles et qui devront être acceptées préalablement à l'utilisation de ces services. Les services sont fournis de manière indépendante par chaque prestataire. Le Client est informé que la résiliation ou l'expiration du service de Gestion de factures entraîne automatiquement la résiliation des services fournis par ces prestataires.

Le service ne peut être rendu que pour : des documents digitalisés selon un format approprié ; des données rédigées dans l'alphabet latin et/ou contenant une numérotation décimale ; des données issues de documents envoyés à partir des formats de fichiers suivants : .jpg, .jpeg, .png, .tiff, .tif, .gif, .pdf, .txt, .docx, .pptx, .xlsx, .doc, .xls. La Banque ne peut pas garantir l'extraction exacte des données et informations issues de documents envoyés sous d'autres systèmes et/ou formats que ceux évoqués ci-dessus.

Lorsque le Client devra choisir une plateforme de dématérialisation partenaire (PDP), il pourra recourir aux services de IPT Technologie (sous réserve de son immatriculation définitive). Si le Client choisit IPT Technologie, le Client entrera en relation contractuelle directe avec celui-ci conformément à ses Conditions Générales et Politique de confidentialité rendues accessibles et qui devront être acceptées préalablement à l'utilisation de ces services au moment du choix opéré par le Client. Les services « PDP » (en particulier réception et transmission de factures électroniques, production des e-reportings exigés par la législation pour les entreprises assujetties à la TVA et transmission à l'administration fiscale) seront intégrés dans le service de Gestion de factures. Le Client est informé que la résiliation ou l'expiration du service de Gestion de factures entraîne automatiquement la résiliation des services fournis par IPT Technologie en qualité de PDP.

- **Exclusions de responsabilités**

Les exclusions de responsabilité qui suivent sont sans préjudice des autres stipulations en vertu du Contrat.

Le Client reconnait et accepte que la Banque n'est pas responsable des services fournis par des prestataires tiers d'information sur les comptes, également appelés agrégation de comptes (intitulés « Synchronisation des comptes bancaires » dans le service de Gestion de factures) et d'initiation de paiement. En particulier, la Banque ne saurait être responsable des dysfonctionnements de ces services, de la sécurité de ces services, et/ou encore de la fréquence de la mise à jour par

les prestataires tiers des informations restituées dans le service de Gestion de factures de l'Espace de banque à distance du Client.

Le Client reconnait et accepte que la Banque n'agit, dans le cadre de la fourniture de ces services, ni en qualité de conseiller, ni en qualité de comptable et que le service ne constitue pas des conseils financiers. Le Client est seul responsable du respect de ses obligations comptables et fiscales, en ce compris de ses obligations de conservation des données comptables et fiscales, et plus généralement des obligations imposées par la règlementation française et européenne.

- **Souscription du service de Gestion de factures et modification du niveau de service**
  Le Client souscrit le service en choisissant le niveau de service avec la tarification associée, adapté à ses besoins. Les cinq niveaux de service de Gestion de factures sont mentionnés dans le parcours de souscription, via l'Espace de banque à distance du Client, ainsi que dans les Conditions tarifaires applicables au Client.

  Le Client peut visualiser le niveau de service qu'il a choisi dans la rubrique « Offre détenue » et changer à tout moment de niveau de service en cliquant sur le bouton prévu à cet effet dans cette rubrique.

  La souscription du service et la modification du niveau de service sont effectuées en ligne par le Client et prennent effet immédiatement. Le Client en reçoit la confirmation à l'écran ainsi que par email à l'adresse électronique communiquée par le client à la Banque.

  La Banque se réserve la possibilité de refuser la souscription du service en cas de souscriptions ou de résiliations successives multiples.

- **Conditions tarifaires**
  Le service est souscrit sous forme d'abonnement mensuel dont le montant est fonction du niveau de service choisi. Le Client pourra accéder aux différentes fonctionnalités incluses dans le niveau de service choisi et dans les limites qu'il prévoit. En cas de dépassement de ces limites : nombre de factures et/ou du nombre d'utilisateurs pour les notes de frais et/ou nombre de banques inclus dans la synchronisation des comptes bancaires prévues dans le niveau de service souscrit, des frais supplémentaires seront facturés. Le Client peut suivre sa consommation directement depuis le service et a la faculté de changer de niveau de service à tout moment.

  La tarification du niveau de service et les frais additionnels en cas de dépassement des limites, sont définis aux Conditions tarifaires de la Banque applicables au Client, disponibles dans la brochure tarifaire accessible depuis le site internet de la Banque ou auprès de l'agence.

  L'abonnement sera facturé mensuellement, à terme échu, à la date anniversaire de la souscription du service. Les éventuels frais additionnels en cas de dépassement des limites seront facturés à terme échu le mois suivant.

- **Durée et résiliation du service de Gestion de factures**
  Le service est souscrit pour une durée indéterminée.

  Le Client peut mettre fin au service à tout moment et sans frais, en contactant l'assistance du service de Gestion de factures via son Espace de banque à distance pour formaliser sa demande de résiliation.

  La résiliation du service interviendra à la date anniversaire de la souscription du service.

  La Banque peut également résilier le service à tout moment. Le Client en sera informé par lettre recommandée avec avis de réception. Cette résiliation prendra effet un mois après l'envoi de cette information.

  Le Client est informé que la résiliation du Service de banque à distance ne permet plus d'accéder au service de Gestion de factures, et entraîne sa résiliation automatique.

  Après la résiliation du service, il ne sera plus possible de l'utiliser, notamment aucun document ne pourra plus être numérisé ni téléchargé. Il appartient donc au Client de procéder à la sauvegarde des documents nécessaires avant la résiliation effective du service.

2.2 - CE net Remises

CE net Remises permet au Client d'effectuer, par l'intermédiaire des Personnes habilitées à utiliser le Service, les principales fonctionnalités décrites ci-après (la liste n'étant pas exhaustive). En souscrivant à l'offre CE net Remises, le Client a accès à l'ensemble des fonctionnalités présentes dans l'offre CE net Comptes.

2.2.1 - Gestion des accès aux Services CE net Remises (saisie, dépôt et relevés)

L'accès des Utilisateurs à CE net Remises est paramétré lors de la souscription dans les Conditions Particulières mais aussi via son espace personnel CE net à partir de l'onglet « Paramétrage », en cliquant sur « gestion des utilisateurs ».

2.2.2 - Déposer et récupérer des fichiers EDI au format CFONB ou variable XML

CE net Remises permet le dépôt de remises de fichiers d'ordres de paiement sur le serveur EDI de la Banque et la récupération de fichiers de données informatisées (relevés de comptes, relevés d'opérations, accusé réception de fichiers, ...) conformes aux standards retenus par le CFONB.

2.2.3 - Saisir et gérer des fichiers EDI en ligne et prestations connexes

CE net Remises permet la saisie, la gestion et le suivi en ligne de fichiers de données informatisées, ainsi qu'un ensemble de prestations connexes :

- l'enregistrement des comptes des destinataires d'opérations,
- la création de listes de destinataires,
- la saisie et le contrôle des remises d'ordres de paiement et leur transfert à la banque,
- l'enregistrement et la modification d'une remise sauvegardée,
- la reprise des effets enregistrés en portefeuille en LCR,
- l'enregistrement des LCR/BOR détenus avant leur transfert dans une remise d'escompte ou d'encaissement,
- la création de listes de mandats de prélèvements SEPA,
- la saisie et le contrôle des remises de prélèvements SEPA à partir de liste de mandats préalablement enregistrés (cf.2.2.4),
- le suivi et la signature des ordres : la visualisation du fichier émis, le contrôle de son état, sa confirmation et sa suppression,
- le Parafeur : la confirmation des ordres par Signature électronique (Cf. article 5),
- la personnalisation de la dénomination d'un compte émetteur et du rang de présentation pour la saisie d'opérations.

2.2.4 - Gérer des mandats et créer des remises de prélèvements SEPA

CE net Remises permet la gestion des mandats de prélèvements SEPA :

- création et modification des mandats par saisie du Client ou par import des données du Mandat,
- génération manuelle ou automatique de la Référence Unique de Mandat (RUM),
- gestion des amendements liés aux modifications des données du mandat,
- gestion des rejets,
- création de listes de mandats de prélèvements SEPA,
- Création de base de mandats, pouvant être partagée entre différents Utilisateurs d'un même abonnement CE Net et habilités à saisir des prélèvements SEPA,
- création des remises de prélèvements SEPA à partir des listes de mandats, regroupées par date d'échéance.

Le Client aura préalablement signé la Convention d'émission des prélèvements SEPA CORE ou SEPA B2B (inter-entreprises).

Les mandats saisis ou importés par le Client dans le cadre des fonctionnalités du Service ainsi que les prélèvements saisis sont sous la responsabilité exclusive du Client. Le Client reconnait que la Banque n'est tenue à cet égard à aucun contrôle ou vigilance particulière. A ce titre, la Banque ne peut être tenue responsable des conséquences financières qui résulteraient d'une mauvaise indication des montants et/ou des comptes de destinataires, des mandats des ordres ou de rejet lors de la présentation des prélèvements à la banque destinataire.

En tout état de cause, le Client fait son affaire des litiges l'opposant à ses débiteurs, la Banque étant dégagée de toute responsabilité à cet égard.

La Banque s'engage à mettre à disposition de ses Clients un service de Gestion de Mandats et de création des prélèvements SEPA conforme aux règles édictées par l'EPC (European Payments Council) et le CFONB.

Pour bénéficier du service de gestion de mandat SEPA, le Client signera les conditions particulières adaptées qui préciseront, notamment, les fonctionnalités choisies ainsi que la tarification applicable.

2.3 - CE net EDI

CE net EDI est une offre à la « carte » proposant au Client de disposer de tout ou partie des Services CE net Remises et de réaliser ses opérations via un protocole de communication bancaire EBICS, SWIFTNet FileAct ou Pe SIT hors SIT moyennant la signature préalable d'un contrat spécifique à ces derniers par acte séparé.

CE net EDI permet aussi au Client de bénéficier du Collège de signature pour les opérations via un protocole de communication bancaire, sur simple demande de sa part. Le service Collège de signature, est un service permettant à l'Abonné d'inclure au sein d'un Collège un ou plusieurs Utilisateurs, permettant ainsi de déterminer les modalités de signature par le jeu de la composition des Collèges et des droits en cosignature.

Pour chaque opération déterminée, un seul Utilisateur par Collège de signature peut signer. La cosignature nécessite la signature de deux Utilisateurs de Collèges différents. Chaque Collège bénéficie des droits de signature définis par le Client.

Les droits des Utilisateurs et du ou des Collèges de signature seront définis dans les Conditions Particulières pour chacun des Services autorisés dans le périmètre de l'abonnement du Client CE net.

Par ailleurs, des Conditions Particulières spécifiques peuvent exister dans le cadre de certaine typologie de clientèle ou de volume de comptes très important.

2.4 - CE net COPRO

Dans le but de faciliter les échanges de documents et l'instruction des dossiers de financement de prêts collectifs copropriété en toute sécurité et confidentialité, la Banque met en œuvre une plateforme d'instruction et transfert de documents « CE net COPRO ». Cette plateforme permet aux syndics de copropriété de monter les dossiers de demande de financement de travaux dans le périmètre de leur abonnement.

ARTICLE 3 - PERSONNES HABILITÉES À UTILISER LE SERVICE

L'ensemble des Personnes habilitées qui sont mandatées à l'effet d'administrer des droits et/ou à l'effet d'utiliser CE net sont désignées aux Conditions Particulières et, le cas échéant, aux annexes du Contrat. L'Utilisateur Principal et les Administrateurs équipés d'un moyen d'Authentification forte, peuvent administrer les droits des Utilisateurs désignés aux Conditions Particulières.

Il est précisé que ces autorisations valent délégation de pouvoirs spécifiquement applicables au Contrat quels que soient les pouvoirs communiqués par ailleurs à la Banque, cette dernière n'ayant pas d'autres contrôles à effectuer.

La liste des Personnes habilitées est accessible à l'Utilisateur Principal et aux Administrateurs, lors de l'utilisation de CE net.

L'ajout, la suppression et/ou le changement de profil d'une Personne habilitée peut faire l'objet de la signature d'un avenant aux Conditions Particulières.

Le Service ne pourra pas être opérationnel pour une personne qui n'a pas été désignée dans la liste.

En cas d'ajout d'une Personne habilitée, il sera alors délivré à cette dernière un numéro d'Utilisateur, un code confidentiel et un dispositif d'Authentification forte utilisables dans les conditions du Contrat.

Il appartient au Client et/ou à l'Utilisateur Principal et/ou à l'Administrateur d'informer la personne dont l'habilitation a été supprimée ou modifiée.

3.1 - L'Utilisateur Principal

L'Utilisateur Principal, désigné aux Conditions Particulières du Contrat :

- A la possibilité (i) d'accéder à tous les Services proposés par la Banque dans le cadre de CE net comptes et CE net Remises, et compris dans le périmètre de l'abonnement prévu aux Conditions Particulières du Contrat, (ii) d'ajouter de plein droit (sans habilitation nécessaire) un nouveau Compte destinataire. L'Utilisateur Principal a tous les droits sur la gestion du Référentiel et des listes de Comptes destinataires,
- Est limité le cas échéant par les plafonds standard de saisie de virements établis par la Banque (ces plafonds sont susceptibles d'évolution et peuvent être modifiés par la Banque à tout moment) ou par les plafonds personnalisés qui peuvent être prévus aux Conditions Particulières sous réserve d'acceptation de la Banque.

De plus, il ne lui est pas possible d'agir sur le périmètre de l'abonnement sauf s'il est le représentant légal du Client ou dûment mandaté à cet effet par le Client.

L'Utilisateur Principal bénéficie également de toutes les fonctions d'Administrateur.

3.2 - L'Administrateur

Le ou les Administrateurs, désigné(s) aux Conditions Particulières du Contrat, ont en charge, sous réserve de disponibilité, l'ajout de nouveaux Utilisateurs et/ou l'attribution des droits aux Utilisateurs sur leur espace personnel CE net dans la limite du périmètre de l'abonnement indiqué aux Conditions Particulières et dans les limites des fonctions accessibles en ligne.

L'Administrateur peut :

- Consulter en ligne l'ensemble des Personnes habilitées à utiliser le Service et désignées aux Conditions Particulières,
- Gérer en ligne (affectation/modification/suppression) les droits des Utilisateurs sur les comptes du périmètre de l'abonnement, sur les fonctionnalités et le cas échéant sur les plafonds d'opérations. Lorsque la gestion des droits s'effectuera en prenant attache auprès de la Banque, de nouvelles Conditions Particulières devront être signées et annexées au présent contrat.
- Créer des Utilisateurs (sous réserve de disponibilité). La création d'un Utilisateur nécessite, auparavant de fournir à la Banque l'ensemble des documents requis que celle-ci pourra demander et de convenir avec la Banque du moyen d'authentification fort pour ce nouvel Utilisateur. Cette création est réalisée au travers de l'espace personnel CE net de l'Administrateur.
- Réaffecter en ligne un nouveau code confidentiel à la suite d'un blocage du code d'un Utilisateur.

Un Administrateur peut par ailleurs être également désigné Utilisateur (profil Administrateur Utilisateur). L'Administrateur Utilisateur bénéficie des fonctions d'Administrateur (article 3.2) et d'Utilisateur (article 3.3) sans pouvoir auto-administrer ses droits.

Ses droits sont gérés en ligne via CE net (Menu gestion des habilitations) par l'Utilisateur Principal, ou un autre Administrateur, ou le cas échéant paramétrés par la Banque à la suite de la demande du Client, formalisée par un avenant au contrat.

3.3 - Les Utilisateurs

Les Utilisateurs, désignés aux Conditions Particulières du Contrat, ne peuvent agir que dans le périmètre qui leur a été dévolu et dans les limites des fonctions accessibles en ligne. Leurs droits sont gérés en ligne via CE net (Menu gestion des habilitations) par l'Utilisateur Principal, ou un Administrateur, ou le cas échéant paramétrés par la Banque à la suite de la demande du Client, formalisée par un avenant au contrat.

L'Administrateur ou l'Utilisateur Principal a la possibilité de demander à la Banque de bloquer temporairement un Utilisateur.

Le Client peut également désigner ses collaborateurs porteurs de carte bancaire à usage professionnel en qualité d'Utilisateurs de CE net afin que ces derniers puissent réaliser, via un dispositif d'Authentification forte, des opérations de paiement par carte bancaire sur internet. Dans ce cadre précis, le Client reconnait que ces Utilisateurs n'auront accès à aucun des Services proposés par CE net à l'exception du module changement de mot de passe, de la Messagerie Sécurisée Internet et du dispositif d'Authentification forte Sécur'Pass Pro.

3.4 - Habilitation à la gestion du référentiel des Comptes destinataires

Il est possible aux Personnes habilitées équipées d'un moyen d'Authentification forte, de gérer le Référentiel des Comptes destinataires (ajout/modification/suppression).

Tous les Comptes destinataires vers lesquels des opérations peuvent être initiées sont enregistrés dans un Référentiel qui peut être consulté en ligne globalement ou partiellement par les personnes qui y sont autorisées. Ce Référentiel peut être composé, le cas échéant, de listes de comptes accessibles à condition d'y avoir été autorisé.

Le profil de chaque Utilisateur pour la gestion, l'utilisation et la consultation des Comptes destinataires est défini par l'Utilisateur Principal ou les Administrateurs dans le cadre de la gestion des habilitations. L'Utilisateur Principal bénéficie systématiquement du profil « Gestion du Référentiel et des listes ».

Trois profils de gestion et d'utilisation de ce Référentiel existent :
- Gestionnaire du Référentiel et des listes (Gestion du Référentiel) :
  - Utilisation et consultation de tous les Comptes destinataires du Référentiel,
  - Gestion du Référentiel et des listes de Comptes destinataires :
    - ajout/suppression de Comptes destinataires,
    - gestion des listes des Comptes destinataires et de leur attribution en consultation ou gestion des Utilisateurs, avec export possible du Référentiel (fichier au format csv).

- Utilisateur du Référentiel et des listes autorisées (Consultation du Référentiel) : Utilisation et consultation de tous les Comptes destinataires du Référentiel, avec en complément, accès aux listes sur lesquelles la personne a été autorisée par le gestionnaire du Référentiel et des listes.

- Utilisateur limité aux listes autorisées (Consultation des listes) : Utilisation et consultation uniquement des listes de Comptes destinataires sur lesquelles la personne a été autorisée par le gestionnaire du Référentiel et des listes.

Le Client garde la possibilité de demander par écrit à la Banque d'ajouter ou de supprimer des Comptes destinataires au périmètre de l'abonnement. Il devra fournir à la Banque, une demande d'enregistrement ou de mise à jour selon un formulaire mis à disposition par la Banque, reprenant notamment les coordonnées bancaires complètes des destinataires. Dans ce cas, la prestation pourra être soumise à tarification.

L'utilisation de profils de gestion permet d'assurer une sécurité concernant l'ajout/la modification/la consultation du Référentiel et/ou des listes. Il est ainsi possible d'habiliter des personnes uniquement à la fonction gestion du Référentiel des comptes destinataires afin d'assurer une sécurité lors de la saisie d'ordres.

Toutefois, il appartient au Client de s'assurer de l'authenticité des coordonnées bancaires qu'il reçoit avant toute intégration dans son Référentiel.

ARTICLE 4 - MOYENS MATÉRIELS ET TECHNIQUES D'ACCÈS À CE NET

4.1 - Principes

Le Client fait son affaire personnelle de l'acquisition ou de la location, de l'installation et de la connexion, de l'entretien et plus généralement de la garde de son matériel et de tous ses moyens techniques d'accès aux réseaux ou logiciels autres que ceux placés sous contrôle exclusif de la Banque ainsi que de leur protection au moyen d'un « Pare-feu » et / ou d'un antivirus à jour. Il en dispose sous son exclusive responsabilité. La Banque n'est pas responsable de l'évolution des logiciels, de leur mise à jour et du maintien des référencements.

Le Client doit assurer la sécurité et la confidentialité des données de son système d'information (comme par exemple, référentiel fournisseurs / référentiels Clients, etc..). Lors de toutes modifications de coordonnées bancaires de ses débiteurs, le Client s'assurera de l'exactitude de ces dernières.

Chacune des parties s'engage à communiquer à l'autre partie tout élément de nature à modifier les conditions de la réalisation de la prestation conformément aux dispositions stipulées dans les Conditions Particulières. Les parties réaliseront des tests préalables à la suite de ces modifications pour s'assurer de la continuité du Service.

4.2 - Logiciel de communication bancaire ou de paiement (EDI et API)

Le Service est accessible par un matériel compatible avec les normes télématiques (notamment, celles du centre serveur de la Banque) et Internet (ordinateur multimédia, téléphone compatible...), et leurs évolutions futures, relié au réseau de télécommunications.

Il appartient au Client de se procurer à ses frais et sous sa responsabilité les matériels et équipements appropriés (modem, cartes et logiciels de communication, logiciel d'agrégation et d'initiation de paiement...) ainsi que les moyens de communication (abonnements, accès à Internet...) nécessaires pour la transmission des ordres et la réception des relevés sur ses équipements.

Préalablement à tout échange de données informatisées et quel que soit le protocole utilisé, une phase d'initialisation est nécessaire pour assurer leur sécurité.

4.3 - Paramétrages et formats de fichier

Il appartient au Client de :

- se conformer aux paramétrages transmis par la Banque pour initier la communication bancaire,
- respecter les formats de fichiers selon la norme CFONB/NUG ou communiqués par la Banque, afin que leur syntaxe soit correcte. Ces formats, susceptibles d'évolutions à tout moment, sont disponibles auprès de votre Banque.

ARTICLE 5 - CONDITIONS D'ACCÈS ET DE SÉCURITÉ DE CE NET

La Banque met à disposition du Client des Instruments de paiement se caractérisant par des dispositifs comportant des Données de sécurité personnalisées et/ou un ensemble de procédures convenu et auxquels le Client a recours pour effectuer ses opérations notamment de paiement.

Chaque Utilisateur doit être équipé d'un dispositif d'Authentification forte requis par la Banque, pour l'accès au Service et son utilisation. Le Client est responsable de l'équipement en dispositif d'Authentification forte de chacun de ses Utilisateurs.

5.1 - Conditions d'accès et d'utilisation

Le Client / l'Utilisateur doit utiliser ses éléments d'identification et les dispositifs d'authentification mis en place par la Banque chaque fois qu'il en reçoit l'instruction, sous peine d'engager sa responsabilité.

La Banque pourra appliquer des exceptions, à l'application de l'Authentification forte, dans les conditions et selon les limitations prévues par le Règlement délégué UE 2018/389 du 27 novembre 2017, en particulier lors de l'accès à CE net et dans le cadre des virements permanents et des virements de compte à compte de l'Abonné.

Pour l'accès au Service, l'utilisation de ce dispositif d'Authentification forte, qui nécessite également la saisie d'un code spécifique, sera exigée par la Banque lors du premier accès et au moins tous les 180 (cent quatre-vingts) jours.

5.1.1 - Accès par code confidentiel

A) PRINCIPE

Les Personnes habilitées accèdent au Service après s'être identifiées par la composition d'une triple clé formée du numéro d'Abonné (identifiant Client), d'un numéro d'Utilisateur et du code confidentiel.

Le numéro d'Abonné est attribué au Client et un numéro d'Utilisateur est fourni à chacune des Personnes habilitées désignée aux Conditions Particulières du Contrat par la Banque.

Pour permettre le premier accès au service, un code confidentiel provisoire est communiqué aux Personnes habilitées (soit par la Banque, soit par l'Utilisateur principal ou l'Administrateur dans le cas où les habilitations d'un Utilisateur sont gérées en ligne). Elles sont tenues de modifier ce code confidentiel provisoire par un code confidentiel qu'elles choisissent, lors de leur première connexion, selon la procédure indiquée par le Service. Ce mot de passe pourra être modifié, à tout moment, par la Personne habilitée à sa seule initiative et par la Banque pour des mesures de sécurité.

Après plusieurs tentatives infructueuses de composition du code confidentiel le dispositif d'accès au Service devient inopérant :

- lorsque le blocage concerne un Utilisateur, l'Utilisateur Principal et le ou les Administrateurs a (ont) alors la possibilité de procéder en ligne, à l'attribution d'un nouveau code confidentiel à l'Utilisateur. Une demande peut aussi être effectuée auprès de la Banque,
- lorsque le blocage concerne un Administrateur, l'Utilisateur Principal et ou les autres Administrateurs ont alors la possibilité de procéder en ligne, à l'attribution d'un nouveau code confidentiel. Une demande peut aussi être effectuée auprès de la Banque,
- lorsque le blocage concerne l'Utilisateur principal, il doit effectuer une demande de déblocage auprès de la Banque.

En cas d'oubli du code confidentiel, l'Utilisateur est invité à suivre le parcours « mot de passe oublié » accessible sur CE net.

B) CONFIDENTIALITÉ DES CODES

Le Client, l'Utilisateur Principal, le(s) Administrateur(s) dans le cadre des droits qu'ils gèrent, doivent informer les Personnes habilitées de leurs obligations de confidentialité découlant du Contrat notamment en leur communiquant les éléments ci-après.

Les Personnes habilitées prennent toute mesure raisonnable pour préserver la sécurité du numéro d'Abonné (identifiant Client), de leur numéro d'Utilisateur et de leur code confidentiel, ainsi que de tout élément d'authentification appartenant aux trois catégories ci-dessus. Les Personnes habilitées s'oblige à les tenir secrets et à ne les communiquer ou les remettre à quiconque, même à la Banque qui ne peut en avoir connaissance et ne les demandera jamais. Par ailleurs, les Personnes habilitées peuvent consulter la page « Sécurité » disponible sur le site Internet de la Banque.

Les Personnes habilitées doivent renouveler leur code confidentiel tous les 24 (vingt-quatre) mois. Il est conseillé de ne pas choisir un code confidentiel aisément décelable par un tiers (tel qu'une date de naissance par exemple).

Le numéro d'Utilisateur et le code confidentiel sont personnels aux Personnes habilitées. Elles en assument la garde, les risques, la conservation et la confidentialité, cela même à l'égard des salariés du Client ou des membres de leur famille. Ceci est une condition déterminante pour sécuriser les relations entre le Client et la Banque.

Toute personne qui en fera l'utilisation sera donc réputée autorisée par le Client et toutes les opérations seront réputées faites par lui. La Banque ne peut pas être tenue pour responsable en cas d'usage frauduleux ou abusif.

Il incombe au Client et aux Personnes habilitées de prendre les mesures nécessaires afin que la confidentialité de ces codes soit préservée et éviter ainsi toute fraude ou abus éventuel. Aussi, les Personnes habilitées doivent changer immédiatement leur code confidentiel, dès qu'elles ont connaissance de la perte, du vol, du détournement ou de l'utilisation frauduleuse de ce dernier, ou en cas de doute quant à la préservation de sa confidentialité, selon la procédure indiquée par le Service.

La Banque, l'Utilisateur Principal et les Administrateurs n'ont pas connaissance du code confidentiel que la ou les Personnes habilitées auront choisi. Néanmoins, l'Utilisateur Principal, et l'Administrateur, dans le cadre du périmètre d'habilitations qu'ils gèrent, peuvent, modifier le code confidentiel d'une personne habilitée, en cas de blocage ou du vol du code confidentiel de cette dernière en leur affectant un nouveau code confidentiel provisoire.

Cette obligation de confidentialité concerne également les codes à usage unique que l'Utilisateur serait amené à utiliser dans le cadre de la réalisation d'opérations nécessitant le recours à l'Authentification forte.

5.1.2 - Accès et validation par Authentification forte - Signature électronique des Opérations sensibles

Conformément à la réglementation en vigueur, la Banque met à la disposition du Client des moyens d'Authentification forte permettant d'accéder à CE net et d'y effectuer des Opérations sensibles avec un niveau de sécurité renforcée.

Le Client est dans l'obligation d'utiliser des moyens d'Authentification forts connus de la Banque et identifiés au Contrat, y compris aux fins d'utilisation de la Signature électronique pour ces opérations.

L'Authentification forte peut s'effectuer soit directement lors de la connexion au Service, puis lors de la validation des Opérations sensibles, soit uniquement lors de la validation des Opérations sensibles, si la connexion au Service a été réalisée par code confidentiel.

A) OPÉRATIONS SENSIBLES DE CE NET

Les Opérations sensibles de CE net sont les suivantes (sous réserve d'y être habilité) :

- ajout / suppression en ligne de nouveaux Comptes destinataires à la liste des Comptes destinataires déjà existants au Référentiel (gestion du Référentiel) ;
- gestion des habilitations en ligne par l'Utilisateur Principal ou par l'Administrateur ;
- commande en ligne des chéquiers (selon option des Caisses) ;
- validation d'un ordre de virement ;
- signature des remises d'ordres.

La liste des Opérations sensibles ci-dessus n'est pas exhaustive et est susceptible d'être complétée ou modifiée à tout moment par la Banque.

B) UTILISATION D'UN LECTEUR CAP

L'utilisation du service Sécurisation des Opérations en Ligne (SOL) par lecteur CAP pour s'authentifier et signer électroniquement une opération, le cas échéant, permet au Client de sécuriser les opérations effectuées en ligne.

La Banque préconise au Client de souscrire au service SOL par lecteur CAP par contrat séparé afin de sécuriser l'Authentification des Utilisateurs et les opérations effectuées en ligne notamment les Opérations sensibles indiquées ci-dessus. Les dispositions du contrat SOL par lecteur CAP viennent compléter celles du contrat CE net.

Les personnes amenées à utiliser SOL par Lecteur CAP doivent être habilitées par le Client à la fois dans le cadre de CE net et dans le cadre du contrat SOL.

C) UTILISATION D'UN CERTIFICAT ÉLECTRONIQUE

Les personnes autorisées par le Client peuvent s'authentifier et le cas échéant signer électroniquement dans le cadre du Service les opérations par l'usage d'un Certificat électronique dont elles ont fait l'acquisition par contrat séparé.

L'utilisation de ce Certificat nécessite l'installation du connecteur de sécurité TurboSign sur l'un des navigateurs internet compatibles : Firefox, Edge, Chrome.

L'Utilisateur du Certificat peut, avec ce Certificat et s'il y a été habilité dans le cadre du Service, réaliser des Opérations sensibles prévues par le Service CE net notamment celles mentionnées ci-dessus.

Une personne habilitée équipée d'un Certificat distribué par la Banque et enregistré dans les systèmes de cette dernière pourra l'utiliser dans le cadre des Services en ligne de CE net sans que le Client ait besoin d'en formaliser la demande auprès de la Banque.

Le Certificat électronique, s'il n'est pas souscrit auprès de la Banque, devra être au standard international en vigueur et faire partie de la liste des autorités de certification reconnues par la Banque et le cas échéant, être déclaré en annexe aux Conditions Particulières des présentes pour pouvoir être pris en compte par le Service (annexe « Déclaration de Certificat électronique »).

Le Client fait son affaire personnelle de la gestion (commande, renouvellement, révocation...) de son Certificat auprès de l'autorité de certification émettrice.

Le Client s'engage à informer, dans les meilleurs délais, par courrier recommandé AR, la Banque de tout changement de porteur du Certificat ou d'habilitation de ce dernier. Dans les 10 (dix) jours qui suivent la réception du courrier AR, une nouvelle déclaration de Certificat conforme sera signée entre les parties. Cette information s'applique également en cas de Certificats électroniques non nominatifs (tels que le Certificat 3Skey),

La Banque ne pourra être tenue responsable des conséquences liées à l'indisponibilité ou à la défaillance du Certificat électronique du Client.

La responsabilité de la Banque ne pourra en aucun cas être engagée en cas d'utilisation du Certificat par un porteur dont l'Identification ou l'habilitation ne lui a pas été communiquée dans les conditions susvisées.

Le Client s'engage à respecter les modalités d'utilisation d'un Certificat lors d'une Authentification forte ou de la Signature électronique, comme suit :

- Le Client ne doit introduire son Certificat sur son poste de travail qu'au moment où l'application d'Authentification ou de signature le demande et doit le retirer dès que l'Authentification ou la signature a été acceptée,
- En aucun cas, le Client ne doit laisser en permanence ou durant toute la durée de travail, le Certificat connecté à son poste de travail.

D) UTILISATION DE SOL SMS

L'utilisation du service SOL SMS pour s'authentifier, valider et/ou signer électroniquement une opération, le cas échéant, permet au Client de sécuriser les opérations effectuées en ligne.

Les Utilisateurs amenés à utiliser SOL SMS doivent être habilités par le Client dans le cadre de CE net.

La liste des fonctionnalités offertes par SOL SMS est susceptible d'évolution. Le Client et l'Utilisateur habilité en sont informés via la documentation s'y rapportant.

E) UTILISATION DE SECUR'PASS PRO

Le Client a accès depuis l'Application mobile, à Secur'Pass Pro, dispositif d'authentification forte permettant notamment au Client :

- d'accéder à CE Net et à son(ses) compte(s) courant(s) en ligne,
- de sécuriser l'accès et l'utilisation de certains services,
- de valider certaines Opérations sensibles initiées depuis son Espace de Banque à distance,
- de valider des opérations de paiement réalisées en ligne (virements) sur son Espace de Banque à distance et des opérations de paiement réalisées par carte bancaire sur internet (e-commerce),
- de s'authentifier lors de la souscription de produits et services commercialisés par la Banque par voie dématérialisée en ayant recours à un dispositif de signature électronique.

La liste des fonctionnalités offertes par Sécur'Pass Pro est susceptible d'évolution. Le Client en est informé via l'Application mobile ou via la documentation s'y rapportant.

Sécur'Pass Pro complète ou se substitue, le cas échéant, aux autres modes d'authentification.

L'enrôlement à Sécur'Pass Pro est effectué par le Client par la saisie de certains numéros de sa carte bancaire ou de sa carte Sécur'Accès en cours de validité et active, détenue auprès de la Banque, ou, dans le cas où il ne dispose pas de carte, par une demande formulée auprès d'un conseiller en agence. Le Client doit posséder un smartphone compatible et un numéro de téléphone mobile préalablement déclaré à la Banque en tant que téléphone sécurisé. Afin d'utiliser Sécur'Pass Pro, le Client doit également activer le service à partir de son Espace de banque à distance accessible depuis l'Application mobile. L'activation de Sécur'Pass Pro nécessite la saisie par le Client d'un code Sécur'Pass Pro qu'il a choisi.

Le changement de smartphone initialement enregistré et/ou la réinstallation de l'application mobile de la Banque nécessite l'enrôlement du nouvel appareil ou un nouvel enrôlement à Secur'Pass Pro.

Le choix, l'enregistrement, la modification, la réinitialisation et la conservation du code Sécur'Pass Pro sont de la responsabilité du Client. Il lui appartient notamment de veiller à le conserver strictement secret, au même titre que l'ensemble des identifiant/mot de passe liés à son Espace de banque à distance ou à ses moyens de paiement. La Banque n'a aucun accès à ce code Sécur'Pass Pro.

Il est conseillé au Client de changer son code Sécur'Pass Pro fréquemment, de ne pas choisir un code Sécur'Pass Pro simple aisément décelable par un tiers, et de ne pas choisir un code Sécur'Pass Pro identique à celui qu'il utiliserait déjà par ailleurs, par exemple, le code PIN associé à son smartphone ou à sa carte SIM, ou le code confidentiel lié à son accès à l'Espace de Banque à distance, ou le code associé à sa carte bancaire.

Lors de l'utilisation de Sécur'Pass Pro, la saisie du code Sécur'Pass Pro pourra éventuellement être effectuée par le Client en utilisant la fonction biométrique de son smartphone.

Le Client a la possibilité de supprimer le dispositif Sécur'Pass Pro à tout moment depuis l'application mobile. En cas de cession de son smartphone, il lui appartient de veiller à la suppression de Sécur'Pass Pro et à la désinstallation préalable de l'application mobile de la Banque.

La suppression de Sécur'Pass Pro est susceptible d'empêcher l'accès à certains services nécessitant le recours à une authentification forte, ou d'entraîner l'application d'exigences ou de délais complémentaires pour la réalisation de certaines opérations.

Pour pouvoir à nouveau accéder au dispositif Sécur'Pass Pro, le Client devra procéder à un nouvel enrôlement.

La suspension ou la fermeture de l'accès à Sécur'Pass Pro pour quelque raison que ce soit, à l'initiative du Client ou de la Banque, entraîne l'impossibilité d'utiliser le dispositif Sécur'Pass Pro et les fonctionnalités liées.

F) SERVICE DE SIGNATURE ÉLECTRONIQUE

L'utilisation du service « Signature électronique » est liée à la détention d'un dispositif d'Authentification forte. Dans le cadre du processus de Signature électronique par un dispositif d'Authentification forte, celui-ci reprend les fonctions d'Authentification et de consentement de la signature auxquels est ajouté un procédé fiable de signature « à usage unique ou à la volée », garantissant le lien entre la Signature électronique et l'acte auquel elle s'attache. Ainsi, dans le cas où le Client transmet un ordre de paiement par l'intermédiaire de CE net (service CE net Remises ou protocole), il devra nécessairement apposer sa « Signature électronique » par l'intermédiaire du service Parafeur du service Signature électronique des ordres.

Les personnes autorisées par le Client à confirmer des ordres pour le compte de ce dernier par un dispositif d'Authentification forte sont indiquées en annexes des Conditions Particulières.

Il est précisé que ces autorisations valent délégation de pouvoirs spécifiquement applicables à la présente Convention quels que soient les pouvoirs communiqués par ailleurs, la Banque n'ayant pas d'autres contrôles à effectuer que le respect des délégations indiquées en annexes des Conditions Particulières.

G) MODALITÉS ET CONDITIONS D'ACCÈS AU SERVICE DE BANQUE À DISTANCE DEPUIS UN SERVICE EN LIGNE FOURNI PAR UNE ENTREPRISE TIERCE ET AUTORISATION DE PARTAGE DE DONNÉES

- Conditions d'accès

Sous réserve de disponibilité, la Banque permet au Client d'accéder à certaines fonctionnalités/opérations (notamment réalisation de virements unitaires ou groupés, ajout d'un bénéficiaire de virement, consultation de solde...) depuis un autre service en ligne (site internet / application, logiciel), ci-après dénommé « espace tiers », fourni par une entreprise tierce.

Le Client peut en bénéficier sous réserve des conditions suivantes :

- Le Client doit avoir souscrit un abonnement de banque à distance incluant ce nouveau canal d'échanges avec sa Banque à partir d'un service en ligne fourni par l'entreprise tierce, ce canal d'échanges ayant été mis en place préalablement entre la Banque et l'entreprise tierce ;
- Le Client a souscrit auprès de cette entreprise tierce le service en ligne de cette dernière et il doit également avoir donné son autorisation à l'entreprise tierce de recevoir de la Banque et de transmettre à la Banque ses données personnelles et non personnelles dans le cadre des opérations effectuées sur la banque à distance à partir de l'espace tiers ;
- Le Client a donné son autorisation à la Banque de partager ses données personnelles et non personnelles avec l'entreprise tierce dans le cadre des opérations effectuées sur la Banque à distance à partir de l'espace tiers. Par cette autorisation, le Client active le canal d'échanges avec l'entreprise tierce ;
- En présence de Personnes habilitées à effectuer des opérations dans son Espace de banque à distance, le Client reconnaît que ces derniers pourront autoriser ce partage de données personnelles et non personnelles et activer ce canal d'échanges avec la Banque depuis cet espace tiers pour effectuer des opérations dans le même périmètre qui leur a été imparti.

- Modalités d'accès

Depuis cet espace tiers, le Client / la Personne habilitée a la possibilité d'être redirigé vers une page de la Banque, où il doit s'authentifier avec ses éléments habituels de connexion à l'Espace de banque à distance. Lors de la première utilisation de ce nouveau canal d'échanges avec la Banque, le Client / la Personne habilitée doit autoriser le partage des données personnelles et non personnelles précitées pour activer ce canal d'échanges. Une fois cette étape réalisée, le Client est informé que la Banque peut communiquer à l'entreprise tierce des données personnelles et non personnelles liées aux opérations demandées par le Client / la Personne habilitée. Le Client / la Personne habilitée est informé des catégories d'informations communiquées à l'entreprise tierce, lors de son activation du canal d'échanges.

- Responsabilités

Il appartient au Client dans le cadre de sa relation contractuelle avec l'entreprise tierce de s'assurer que celle-ci n'utilise pas les données partagées pour une finalité autre que de permettre au Client de communiquer avec sa Banque à partir de son espace tiers/service en ligne.

La Banque n'est pas responsable des dysfonctionnements ou de la sécurité du service en ligne de l'entreprise tierce.

La Banque est responsable de la transmission à l'entreprise tierce des données demandées par le Client à partir de son espace tiers et du traitement des données reçues du Client par le biais de son espace tiers.

La Banque n'est pas responsable de la fréquence de la mise à jour par l'entreprise tierce des informations restituées dans l'espace tiers.

5.2 - Obligation des parties

5.2.1 - Obligations du Client

Le Client est responsable de l'équipement en dispositif d'Authentification forte de chacun de ses Utilisateurs, pour l'accès à CE net et, le cas échéant, pour la réalisation des virements et des Opérations sensibles.

Le Client/l'Utilisateur doit utiliser ses éléments d'identification et les dispositifs d'Authentification forte mis en place par la Banque chaque fois qu'il en reçoit l'instruction, sous peine d'engager sa responsabilité.

Toute personne qui en fera l'utilisation sera donc réputée autorisée par le Client et toutes les opérations seront réputées faites par lui. La Banque ne peut pas être tenue pour responsable en cas d'usage frauduleux ou abusif.

Dès qu'il reçoit un Instrument de paiement, le Client prend toute mesure raisonnable pour préserver la sécurité de ses Données de sécurité personnalisées qui sont placées sous sa garde. Il utilise son Instrument de paiement conformément aux conditions régissant sa délivrance et son utilisation et définies ci-après par Service.

5.2.2 - Obligations de la Banque

Lorsqu'elle délivre à un Client un Instrument de paiement, la Banque s'assure que les Données de sécurité personnalisées de cet Instrument ne sont pas accessibles à d'autres personnes que le Client et/ou l'(les) Utilisateur(s) autorisé(s) à utiliser cet Instrument, sauf si le Client/l'Utilisateur ne respectent pas les recommandations et obligations à leur charge.

Elle s'abstient d'envoyer tout Instrument de paiement non sollicité, sauf si un Instrument déjà donné doit être remplacé.

La Banque informera le Client, de façon sécurisée, en cas de soupçon de fraude, de fraude avérée ou de menaces pour la sécurité survenant sur le service CE net.

5.3 - Recommandations spécifiques relatives au Service CE net

Dans le souci de protéger la confidentialité des données bancaires du Client, la Banque, en particulier dans le cadre des règles d'usage d'internet, invite le Client à prendre toute disposition utile, notamment en effaçant, dès la fin de la consultation, les traces de sa navigation et en interdisant l'accès aux tiers non autorisés dans l'hypothèse de leur téléchargement vers un logiciel de gestion.

De façon générale, la Banque rappelle au Client qu'il lui appartient de protéger les données et/ou les logiciels stockés ou chargés, et/ou l'équipement informatique utilisé, de la contamination par des virus ou de tentatives d'intrusion, quelles qu'elles soient.

Le Client est tenu de sécuriser son ordinateur, sa tablette ou son téléphone mobile, au moyen de solutions de sécurité de son choix (verrouillage du téléphone, logiciel anti-virus et anti-espion, Pare-feu ...) et de maintenir ces dispositifs à jour en permanence.

Le Client est ainsi invité à prendre connaissance des mesures à mettre en œuvre afin de sécuriser ses connexions Internet en consultant la page « Sécurité » disponible sur le site Internet de la Banque (www.caisse-epargne.fr).

Dès lors que le Client autorise l'accès en ligne à son compte par un prestataire de service d'initiation de paiement (virements) ou d'information sur les comptes (service d'agrégation de comptes), ce prestataire doit disposer de l'agrément délivré par l'autorité compétente d'un Etat membre de l'Union Européenne ou être inscrit sur le registre tenu par cette autorité, conformément à la règlementation en vigueur. Le Client est tenu de vérifier que ce prestataire dispose de cet agrément ou est inscrit sur le registre concerné. Le Client peut être tenu de communiquer à ce prestataire, sous sa responsabilité, tout ou partie de ses éléments d'identification et d'authentification pour l'accès à CE net.

L'initiation d'opérations de paiement (virements) par ce prestataire, pour le compte du Client, s'effectuera selon les mêmes modalités et conditions d'authentification que si le Client réalisait directement ces opérations par l'intermédiaire de CE net.

ARTICLE 6 - OPPOSITION À L'UTILISATION DES SERVICES EN LIGNE DE CE NET

Le Client s'engage à se rendre immédiatement à son Agence ou à avertir immédiatement la Banque par lettre recommandée avec demande d'avis de réception, ou par tous autres moyens confirmés par lettre recommandée avec demande d'avis de réception, dès qu'il considère que la confidentialité de l'accès au Service n'est plus assurée pour quelque motif que ce soit.

6.1 - Opposition (blocage) à l'accès au Service consécutive à la perte ou vol des éléments d'identification et/ou d'Authenfication forte

Dès qu'ils ont connaissance de la perte, du vol, du détournement ou de l'utilisation frauduleuse des éléments d'identification et/ou d'Authentification forte personnels d'une Personne habilitée, le Client et/ou l'Utilisateur Principal doivent immédiatement en informer par tous moyens la Banque qui bloquera l'accès aux Services en ligne de CE net.

L'opposition devra être immédiatement confirmée par courrier recommandé avec demande d'avis de réception ou directement auprès de la Banque. En cas de contestation, la date de réception de l'écrit fera foi entre les parties.

Les conséquences d'une absence d'opposition sont précisées à l'article 15.4.

6.2 - Opposition à une carte de paiement ou à une carte Sécur@ccès utilisée dans le cadre de SOL par lecteur CAP

Dès connaissance de la perte, du vol ou d'une utilisation frauduleuse d'une carte Sécur@ccès, ou d'une carte de paiement, le Client, son représentant légal ou le porteur devra immédiatement faire procéder au blocage de cette dernière et confirmer par déclaration écrite auprès de la Banque ayant délivré la carte.

Le Client est invité à se référer, pour les conditions d'opposition aux cartes délivrées par la Banque et utilisables dans le cadre du Service, au contrat SOL par Lecteur CAP ou au contrat porteur carte.

La Banque ne saurait être tenue pour responsable des opérations effectuées dans le cadre du Service avec une carte délivrée par la Banque à défaut d'opposition dans les conditions contractuellement prévues.

6.3 - Révocation du Certificat électronique utilisé dans le cadre des Services en ligne de CE net

Dès qu'ils ont connaissance de la perte, du vol, du détournement ou de toute utilisation frauduleuse d'un Certificat électronique, le Client, ou son représentant légal, ou le mandataire de certification, ou encore le porteur du Certificat, doivent révoquer le Certificat électronique auprès de l'Autorité de Certification dans les conditions indiquées au contrat relatif au Certificat électronique souscrit par ailleurs par le Client, aux fins de blocage de ce dernier.

Le Client et/ou le porteur du Certificat en informe sans tarder et par tous moyens la Banque afin de bloquer l'utilisation du Certificat sur le Service.

La personne, dont le Certificat électronique est révoqué, ne peut plus alors s'authentifier et utiliser la fonction de Signature électronique de son Certificat notamment pour accéder aux Opérations sensibles proposées en ligne dans le cadre de CE net.

Toutes les opérations effectuées dans le cadre du Service à l'aide du Certificat électronique par une personne habilitée, avant publication par l'Autorité de certification, sont présumées émaner de ce dernier.

ARTICLE 7 - CONDITIONS D'EXÉCUTION DES OPÉRATIONS ET ORDRES DE PAIEMENT DÉPOSÉS VIA CE NET, TRANSMIS VIA UN TIERS INITIATEUR DE PAIEMENT (API), OU TRANSMIS VIA UN PROTOCOLE DE COMMUNICATION BANCAIRES EDI

Les ordres de paiement et les opérations qui découlent de CE net sont soumis aux conditions de traitement habituelles en vigueur à la Banque, à la date de l'opération et objet de la convention de compte courant régularisée par acte séparé par le Client ou de toutes autres conventions existantes liées à des services spécifiques signées par le Client, ainsi que le cas échéant par les conventions/contrats liés aux différents protocoles utilisés (EBICS, SWIFTNET), sauf conditions spécifiques prévues dans les conditions particulières de la convention de compte courant, et/ou dans les Conditions Particulières du Contrat.

Ainsi, le Client doit vérifier la bonne exécution de ses ordres, notamment lorsqu'ils sont destinés au paiement de sommes dues à date fixe.

7.1 - Dispositions applicables aux remises d'ordres de virements SEPA

Concernant les remises d'ordres de virements SEPA (Classique, Jour, Spécial, Instantané) et les prélèvements SEPA (Core ou Interentreprise), le Client pourra choisir, sous réserve de disponibilité, le mode de comptabilisation de la remise sur le compte donneur d'ordres :

- Comptabilisation Nette : la remise d'ordres traitée sera comptabilisée, sur le compte du Client donneur d'ordre, de la somme totale des ordres transmis sous déduction des ordres écartés selon les contrôles de faisabilité effectués par les systèmes de traitement de la Banque.
- Comptabilisation Brute : la remise d'ordres sera comptabilisée sur le compte du Client donneur d'ordre de la somme totale des ordres transmis. Les ordres qui auront été écartés et non échangés, selon les contrôles de la Banque, seront comptabilisés sur le compte du Client donneur d'ordre dans le sens inverse de la remise des ordres.

La Banque peut être amenée à soumettre les remises d'ordres de virements ou de prélèvements à des limites de plafonds par client. Ces limites peuvent être par ordre unitaire, cumul journalier et cumul mensuel. Dans le cas de dépassement de l'un de ces plafonds, la remise ne sera pas traitée ce dont le Client sera informé.

Fonctionnalité d'anonymisation des informations relatives aux virements de salaires, dans les relevés mis à la disposition du client (sous réserve de disponibilité) :

Pour les fichiers de remises d'ordres SEPA et s'agissant de règlement de virements de salaires, le Client pourra demande d'opter pour la fonctionnalité d'anonymisation des informations relatives aux virements de salaires au niveau des relevés mis à la disposition du Client ou en consultation sur CE net.

Cette fonctionnalité est disponible sur les remises d'ordres virement SEPA (Classique, Jour, Spécial), sous réserve que le Client renseigne à « SALA » la balise « category purpose » dans son fichier d'ordres transmis préalablement (<CtgyPurp>SALA</CtgyPurp>, au niveau lot - Payment Information - de la remise). La Banque anonymisera l'ensemble des informations (Nom, Prénom, Adresse du bénéficiaire).

Par ailleurs, dans le cas où le Client a fait le choix d'une comptabilisation unitaire, l'anonymisation sera aussi appliquée sur le relevé de compte des ordres transmis.

Vérification du bénéficiaire - Virements SEPA déposés sous forme de fichier (Classique, Jour, Spécial, Instantané) (service permettant de renforcer la sécurité des virements et de réduire les risques d'erreurs et de fraudes) **:**

- Principes généraux

Conformément au Règlement (UE) 2024/886 du 13 mars 2024, ce service permet au Client de demander à la Banque d'effectuer une vérification des bénéficiaires de virements SEPA classiques et instantanés, auprès de leur Prestataire de Service de Paiement (PSP). Cette vérification porte sur la concordance entre l'IBAN et le nom du bénéficiaire de virement SEPA. Ce service est fourni au Client à titre gratuit.

- Réalisation de la vérification

Lors de la remise de chaque fichier d'ordres de virements SEPA sous une forme groupée, le Client peut choisir :

- de soumettre ce fichier à la vérification des bénéficiaires ou,
- de bénéficier du service de « Vérification à la demande » ou,
- de renoncer à la vérification des bénéficiaires.

- Renonciation au service de vérification du bénéficiaire

Lors du dépôt de chaque fichier de remise d'ordres de virements SEPA, le Client peut renoncer au service de vérification du bénéficiaire pour le fichier concerné. En renonçant à ce service, le Client est informé que les virements pourraient être crédités sur le compte d'un autre bénéficiaire que celui auquel le Client souhaite transmettre les fonds. Le Client peut décider, à tout moment, de bénéficier à nouveau de ce service, lors du dépôt d'un nouveau fichier de remise d'ordres de virement.

- « Vérification à la demande »

Dans le cas où le Client souhaite que cette vérification des bénéficiaires soit réalisée pour ce fichier, il lui est proposé de demander uniquement la vérification des bénéficiaires, sans exécution des virements, dans le cadre du service « Vérification à la demande », s'il a préalablement souscrit à ce service dans les Conditions Particulières du Contrat.

Après consultation des résultats de la vérification, le Client transmettra un fichier d'ordres de virement pour exécution qui ne fera pas l'objet d'une vérification des bénéficiaires.

Ce service ne peut être utilisé à d'autres fins que la vérification des bénéficiaires au préalable d'une opération de virement SEPA. Le Client s'engage à ne pas utiliser le service de manière à le détourner de sa finalité.

- Résultats de la vérification

Le résultat de la vérification des bénéficiaires est mis à disposition du Client par la Banque, dans le suivi des remises, dans les Relevés et dans le Parapheur, avant signature des ordres. Ce rapport détaille le résultat de la vérification pour chaque bénéficiaire :

- Concordance : le nom associé à l'IBAN correspond au nom du bénéficiaire que le Client a renseigné.
- Concordance partielle : le nom associé à l'IBAN ne correspond pas exactement au nom du bénéficiaire que le Client a renseigné. La Banque communique alors au Client le nom du bénéficiaire associé à l'IBAN qu'il a fourni.
- Non concordance : le nom associé à l'IBAN ne correspond pas au nom du bénéficiaire que le Client a renseigné. La Banque ne lui donne aucune information sur le bénéficiaire.
- Vérification impossible : la concordance entre l'IBAN et le nom du bénéficiaire que le Client a renseigné n'a pas pu être vérifiée. Le Client est également informé si le compte du bénéficiaire est clôturé.

Ce résultat n'est valable qu'au moment de la mise à disposition du rapport par la Banque au Client, et ne saurait en aucun cas prévaloir pour l'avenir.

Une validation des bénéficiaires par le Client sera nécessaire en cas d'anomalie de concordance afin de permettre à la remise de virements de remonter dans le Parapheur en vue de la signature des ordres.

En cas de concordance partielle et de non-concordance, le Client est informé que l'autorisation du virement pourrait conduire à ce que les fonds soient virés sur le compte d'un autre bénéficiaire que celui auquel le Client souhaite transmettre les fonds.

Si, malgré les alertes, le Client autorise le virement, la Banque l'informe :

- Que le virement est considéré comme exécuté au profit du bon bénéficiaire ;
- Qu'elle ne peut pas être tenue responsable de l'exécution de ce virement au profit d'un mauvais bénéficiaire ;
- Qu'il n'a pas droit au remboursement de ce virement pour opération mal exécutée.

7.2 - Dispositions applicables aux LCR/BOR

Le Client peut remettre des LCR et des BOR à l'encaissement, à l'escompte, à titre de garantie d'un crédit ou d'une avance de trésorerie. La confirmation des ordres est réalisée par Signature électronique et de façon exceptionnelle par télécopie.

Lorsque le Client remet des LCR et des BOR à l'escompte, ou à titre de garantie d'un crédit ou d'une avance, il doit avoir préalablement signé une convention-cadre de cession de créances professionnelles ayant pour objet de préciser les modalités d'application de la loi dans ses rapports avec la Banque. Un bordereau de cession de créances (Dailly) doit être corrélativement joint à cette remise.

En tout état de cause, quelle que soit l'option choisie, chaque remise de LCR et/ou de BOR confirmée par Signature électronique doit être accompagnée d'un bordereau de cession de créances Dailly établi à l'ordre de la Banque conformément à la convention cadre de cession de créances. Le bordereau de cession de créances Dailly sera transmis soit par télécopie à la Banque et ce concomitamment au dépôt de la remise, soit confirmé sur CE net par Signature électronique. Dans ce dernier cas, le Client, à la suite de son dépôt de remise de LCR ou BOR, devra confirmer par Signature électronique le bordereau de cession en format PDF, généré à partir des informations contenues dans la remise transmise par le Client.

7.3 - Service de Protection (CE Net Remises et CE Net EDI)

7.3.1 - Contrôle de liste sur pays approuvés

Ce contrôle permet de vérifier la cohérence entre le code pays du destinataire du flux télétransmis et la liste des codes pays destinataires approuvés par le Client. Une limite de montant peut être définie par opération. En cas de divergence l'opération est rejetée.

7.3.2 - Contrôle de liste des Comptes destinataires approuvés

Ce contrôle permet de vérifier la cohérence entre les destinataires du flux télétransmis et la liste des Comptes destinataires approuvés par le Client et par type de remise. En cas de divergence l'opération est rejetée.

ARTICLE 8 - MODALITÉS D'AUTORISATION DES ORDRES DE PAIEMENT

Une opération ou une série d'opérations de paiement est autorisée si le donneur d'ordre a donné son consentement à son exécution ou à l'exécution de la série d'opérations.

8.1 - Transfert de fichiers à l'aide des protocoles EBICS, Pe SIT hors SIT ou le service CE net Remises

Le transfert de fichiers doit faire l'objet d'une confirmation de l'ordre.

Cette confirmation prend la forme d'une Signature électronique, conformément aux habilitations définies en annexes des Conditions Particulières du Contrat ou des protocoles de communication concernés le cas échéant.

Il est précisé que le Client donne mandat à la Banque de procéder à l'exécution de tous les ordres de paiement dont la Signature électronique sera effectuée à l'aide d'un Certificat en cours de validité ou d'un Lecteur CAP selon les modalités décrites à l'article 5.

A titre exceptionnel, en solution de contournement, et avec l'accord de la Banque, la confirmation pourra être transmise par télécopie revêtue de la ou des signatures accréditées préalablement.

Sauf limites stipulées aux annexes relatives aux « habilitations de signature » et/ou aux conventions liées au protocole de communication le cas échéant, les Personnes habilitées par le Client, à remettre et/ou à signer les ordres sont réputées avoir tous pouvoirs. Elles sont donc réputées agir par délégation et sous l'entière responsabilité du Client.

La confirmation de l'ordre doit contenir le type d'opérations transmises, le numéro de compte Banque du donneur d'ordre, le nombre d'opérations, le montant global de la remise, la devise le cas échéant, et la date d'exécution souhaitée.

L'application de cette procédure par le Client vaut consentement de ce dernier à l'exécution de l'opération.

Par ailleurs, à défaut de dispositions contraires spécifiques, la Banque n'exécutera pas les instructions transmises par EDI et confirmées autrement que par Signature électronique, voire, dans les conditions visées ci-dessus, par télécopie notamment celles confirmées verbalement, par téléphone, ou par courriel.

De plus, il est précisé que la Banque est dégagée de toute responsabilité pour l'exécution, une seconde fois, de l'ordre transmis deux fois par le Client :

- par EDI avec confirmation,
- et par courrier ou par télécopie,

sans qu'il soit fait expressément mention qu'il s'agissait du même ordre.

Le fichier EDI transmis par le Client et sa confirmation, soit par Signature électronique sur CE net, soit par Signature électronique jointe au fichier, voire par télécopie, constitueront, sauf preuve contraire, le mode de preuve du contenu et de la transmission des instructions exécutées par la Banque ; ils engageront le Client dans les mêmes conditions et avec les mêmes effets juridiques qu'un écrit comportant une signature manuscrite.

8.2 - Transfert de fichier utilisant le service SWIFTNet FileAct ou SWIFTNet FIN sans signature jointe

Lorsque le Client a choisi aux Conditions Particulières de la convention relative aux protocoles bancaires de confirmer ses ordres par Signature électronique via CE net EDI, les dispositions prévues au Contrat sont applicables.

Lorsque le Client utilise SWIFTNet FileAct ou SWIFTNet FIN sans signature jointe et choisit aux Conditions Particulières de la convention relative aux protocoles bancaires de ne pas confirmer ses ordres par Signature électronique via CE net EDI, les dispositions suivantes sont applicables :

Dès lors que le Client est correctement identifié selon les modalités décrites à la convention SWIFTNet, signée par acte séparé, il est expressément convenu entre les parties que :

- la remise d'ordre est émise par le Client de façon certaine,
- cette Authentification vaut consentement du Client à l'exécution de l'opération.

Le Client prend alors l'entière responsabilité du processus d'émission des ordres à partir de sa station Swift internalisée ou gérée par un prestataire. Il est expressément convenu entre les parties, qu'aucune contestation d'un ordre de paiement émis à partir de son BIC ou le BIC du mandataire pour opération non autorisée ne sera donc admise. Cependant, en cas de déclaration par le Client de la perte ou du vol de l'accès sécurisé SWIFT, une telle contestation pourra être formulée par le Client, dans le cas où cette déclaration aura été faite préalablement à l'Identification du Client et adressée à SWIFT et à la Banque.

ARTICLE 9 - MODALITÉS DE CONFIRMATION DES FICHIERS DE REMISES D'ORDRES DÉPOSÉS VIA LE SERVICE OU TRANSMIS PAR UN PROTOCOLE DE COMMUNICATION BANCAIRE

Les fichiers de remises d'ordres transmises à l'aide des protocoles EBICS - Profil T (transport uniquement), Pe SIT, ou encore saisis ou déposés sur CE net doivent être confirmées par le Client, de façon disjointe par Sécur'Pass Pro, Lecteur CAP ou Certificat électronique en cours de validité. Seules les opérations valides seront proposées à la signature disjointe.

Concernant la confirmation des ordres par Certificat Electronique, celle-ci peut s'effectuer :

- soit de façon jointe au fichier conformément aux dispositions du protocole utilisé : EBICS – profil TS (Transport et Signature jointe) et SWIFTNet FileAct signé,
- soit de façon disjointe via CE net pour les ordres transmis par les protocoles EBICS – profil T (Transport uniquement), saisis ou déposés sur CE net. Seules les opérations valides seront proposées à la signature disjointe.

L'utilisation du Certificat électronique ou Lecteur Cap dans le cadre de la Signature électronique doit être conforme aux conditions décrites à l'article 5 ci-dessus.

Dans le cas contraire, la Banque ne pourra être tenue responsable de la signature par Certificat électronique d'un ordre non autorisé.

Le contenu du fichier doit être validé par le Client avant toute confirmation par Signature électronique.

A titre exceptionnel, en solution de contournement et avec l'accord de la Banque, le Client peut confirmer par télécopie ses saisies ou transferts d'ordres. Toutefois, cette procédure dégrade la sécurité des saisies ou transferts d'ordres et la Banque déconseille au Client d'utiliser ce moyen de confirmation. Dans tous les cas, le Client assumera toutes les conséquences qui résulteraient des risques inhérents aux confirmations par télécopie.

Pour chaque nature d'opérations, la confirmation doit parvenir à la Banque, au plus tard avant les échéances précisées aux Conditions Particulières du Contrat.

ARTICLE 10 - CONDITIONS D'UTILISATION ET DISPONIBILITÉ DU SERVICE

10.1 - Généralités

Le Service est accessible via le réseau Internet 24 heures sur 24 et 7 jours sur 7 sur tout type de supports (ordinateurs, tablettes, smartphones).

Le Service peut être suspendu pour assurer sa maintenance ou sa mise à jour ou pour des motifs non imputables à la Banque, notamment en cas de force majeure ou du fait de tiers tels que les opérateurs de réseaux de télécommunications.

Le Client sera informé par la Banque par tous moyens, des nécessaires périodes de maintenance programmée.

10.2 - Règlement des incidents

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

ARTICLE 11 - PREUVE DES OPÉRATIONS ET DÉLAI DE RÉCLAMATION

Les opérations effectuées par le Client par l'intermédiaire du Service et portées sur le relevé ou arrêté de compte qui lui est adressé, peuvent être contestées par ce dernier dans le délai et aux conditions indiquées dans la convention de compte courant ou, le cas échéant dans la/les conventions liés aux différents protocoles utilisés par le Client (EBICS, SWIFTNET) et signées par ce dernier.

11.1 - Enregistrements

La preuve des opérations effectuées dans CE net pourra être faite par toute forme d'enregistrements résultant des moyens de communication utilisés entre le Client, les Personnes habilitées et la Banque.

Plus particulièrement, la Banque met à disposition du Client un accusé de réception relatif aux échanges effectués :
- via les protocoles de communication bancaire, EBICS et service SWIFTNet FileAct ou SWIFTNet FIN,
- ou via CE net.

De convention expresse, les parties ne reconnaissent que les enregistrements effectués par la Banque, quel qu'en soit
- le support,
- le type ou le montant des opérations réalisées,
- le fichier EDI ou les remises d'ordres,
- la Signature électronique,
- l'accusé de réception,
- les notifications adressées par SWIFT lors de chaque échange,
- les enregistrements réalisés par SWIFT.

Ces enregistrements informatiques (notamment les logs d'échanges et les données reçues) ainsi que leur reproduction réalisée par la Banque, feront foi entre les parties sauf preuve contraire.

11.2 - Preuve du consentement du Client

De convention expresse, la Banque et le Client reconnaissent que :
- l'identification correcte du Client, associé à l'accusé de réception, leur permet de considérer les fichiers comme valablement déposés sur la plateforme informatique de la Banque,
- les fichiers informatiques étant transmis et confirmés par le Client en recourant à l'utilisation de certificats de transport ou de certificats d'Authentification ou de cartes paramètre, celui-ci est réputé en être l'auteur,
- les interrogations ou les ordres sont réputés émaner du Client dès lors qu'ils sont constitués, du numéro du Client, du numéro d'Utilisateur et du code confidentiel, et le cas échéant de l'utilisation d'un Certificat électronique ou d'un moyen d'Authentification forte. Ces éléments constituent une preuve du consentement des opérations sollicitées et/ou réalisées.

11.3 - Récapitulatif des transactions

La preuve des opérations effectuées pourra également être rapportée par tous moyens notamment par les récapitulatifs des transactions établis par les systèmes informatiques de la Banque.

ARTICLE 12 - INTÉGRITÉ, CONFIDENTIALITÉ DU SERVICE

La Banque assure une totale confidentialité des données saisies par le Client dans CE net.

La saisie d'ordres par le Client sera systématiquement chiffrée. Ce chiffrement au moyen d'une clé de cryptage permet d'assurer la confidentialité des échanges. Il appartient au Client de disposer des logiciels permettant ce niveau de protection.

ARTICLE 13 - MODIFICATION DES CONDITIONS PARTICULIÈRES ET DES CONDITIONS GÉNÉRALES DE CE NET

13.1 - Modification du fait de la Banque

La Banque aura la faculté de modifier les Conditions Générales et les Conditions Tarifaires du Service. A cet effet, la Banque communiquera le projet de modification par écrit (par exemple, lettre, mention sur le relevé de compte ou information dans son Espace de banque à distance) au Client, au plus tard un mois avant la date d'application envisagée.

La Banque et le Client conviennent que l'absence de contestation du Client dans ce délai vaut acceptation par ce dernier des modifications. En cas de refus du Client, ce dernier peut résilier sans frais, avant la date d'application des modifications, le Contrat. A défaut de résiliation dans ce délai, les modifications lui seront opposables.

Compte tenu de l'évolution nécessaire et régulière des moyens de sécurité, la Banque se voit expressément reconnaître par le Client, sans recours possible de ce dernier contre la Banque, la possibilité, à tout moment et à effet immédiat, de modifier de façon unilatérale les conditions d'authentification nécessaires à l'accès aux services, ou de supprimer certains dispositifs d'authentification moyennant une information du Client par tout moyen au choix de la Banque.

13.2 - Modifications imposées par des textes législatifs ou règlementaires

Les modifications de tout ou partie du Contrat qui seraient rendues nécessaires par des dispositions législatives ou réglementaires, seront applicables dès leur date d'entrée en vigueur, sans préavis ni information préalable.

ARTICLE 14 - TARIFICATION

Le coût de l'abonnement et la tarification liée aux opérations effectuées seront prélevés sur le (les) compte(s) mentionné(s) dans les Conditions Particulières.

La tarification pourra être révisée à tout moment. Le nouveau tarif sera porté à la connaissance du Client dans les conditions prévues par l'article 13.

Le Client supportera le coût des consommations téléphoniques ainsi que tout montant, redevance, abonnement ou taxes afférentes à l'abonnement téléphonique ou auprès du fournisseur d'accès internet.

14.1 - Coût de l'abonnement

La tarification du Service est composée d'un abonnement forfaitaire mensuel et/ou d'une tarification par service dont le montant est fixé dans les Conditions Tarifaires de la Banque ou aux Conditions Particulières.

14.2 - Tarification des opérations effectuées et des actes de gestion

Par ailleurs, le Client reconnaît avoir été informé que les services et/ou opérations et/ou actes de gestion sollicités et/ou effectués, notamment par l'intermédiaire de CE net, peuvent donner lieu à tarification conformément aux Conditions Tarifaires de la Banque, dont le Client reconnaît avoir pris connaissance et qui sont notamment disponibles dans les agences et sur le site Internet de la Banque.

ARTICLE 15 - RESPONSABILITÉS DE LA BANQUE ET DU CLIENT

15.1 - Responsabilité de la Banque

15.1.1 - Engagements de la Banque

La Banque s'engage à tout mettre en œuvre pour assurer le bon fonctionnement du Service, notamment la bonne exécution des ordres reçus et la confidentialité des informations communiquées.

D'une manière générale, la Banque ne pourra être tenue pour responsable que des dommages ayant pour cause unique son propre fait.

Au cas où la responsabilité de la Banque serait établie, seul le préjudice personnel, prévisible, matériel et direct du Client donnera lieu à réparation.

La Banque ne saurait être tenue pour responsable :

- en cas de non-respect par le Client ou tout Utilisateur des procédures d'utilisation de CE net, en cas de divulgation du ou des codes confidentiels (dont ceux générés par le dispositif d'Authentification forte) à une tierce personne, y compris à un prestataire de service d'initiation de paiement ou d'information sur les comptes, disposant d'un agrément ou d'un enregistrement prévu par les textes en vigueur,
- en cas d'utilisation, par une tierce personne, du Certificat électronique, du service SOL SMS, du service Sécur'Pass Pro, ou de l'Authentification fournie par le service de Sécurisation des Opérations en Ligne par Lecteur CAP (SOL par Lecteur CAP),
- lorsque les informations communiquées par le Client, y compris sur les Utilisateurs, lors de l'adhésion ou lors de l'utilisation de CE net s'avèrent inexactes ou incomplètes,
- en cas de connexion du Client ou de tout Utilisateur à un autre site que le Site légitime et sécurisé de la Banque,
- en cas d'interruption temporaire du Service pendant des périodes courtes pour des raisons techniques et en vue de réaliser des prestations de maintenance ou d'actualisation du Service ou de l'Application mobile de la Banque,
- en cas d'interruption des prestations pour des raisons résultant de la force majeure, du cas fortuit ou du fait d'un tiers,
- des conséquences résultant d'un défaut de sécurité (matériel ou logiciel, antivirus) du terminal de connexion (ordinateur, terminal mobile...) utilisé par le Client ou tout Utilisateur n'ayant pas détecté, notamment, l'intrusion d'un virus informatique.

Sont, notamment considérés comme cas de force majeure :

- Le défaut de fourniture de courant électrique,
- les interruptions de service consécutives au mauvais fonctionnement du matériel utilisé par le Client,
- la défaillance du transporteur d'information ou les incidents affectant les lignes et réseaux de transmission,
- les guerres, émeutes, grèves, incendie...

15.1.2 - Causes d'exemption de la responsabilité de la Banque

La responsabilité de la Banque ne saurait être engagée en raison des conséquences directes et indirectes liées aux mesures, quelles qu'elles soient, notamment gel des avoirs, qu'elle pourrait être amenée à prendre dans le cadre des obligations mises à sa charge par les pouvoirs publics, en particulier au titre de la lutte contre le blanchiment des capitaux et le financement du terrorisme. A ce titre, la Banque ne saurait être tenue pour responsable des retards d'exécution.

La Banque demeure étrangère à tout litige pouvant survenir entre le Client et son prestataire de service d'initiation de paiement ou d'information sur les comptes.

15.2 - Responsabilité du Client quant aux opérations effectuées par les Personnes habilitées dans CE net

Le Client s'engage notamment au respect des conditions d'utilisation du Service, et particulièrement au respect des instructions liées à la sécurité du Service définies dans les Conditions Générales et les Conditions Particulières.

Le Client dégage la Banque de toute responsabilité en cas, par exemple, d'un défaut de traitement d'un fichier en raison du non-respect des contraintes techniques du Service par le Client.

15.2.1 - Délégation responsabilité du Client

L'Utilisateur Principal, s'il n'est pas le Client lui-même, ainsi que les Administrateurs, sont considérés comme expressément habilités par le Client à l'effet de gérer les droits des personnes ayant accès au Service comme indiqué à l'article 3 ci-dessus.

Toute Personne habilitée sera réputée agir par délégation et sous l'entière responsabilité du Client.

Le Client reste tenu des conséquences relatives à la conservation et à la préservation de la confidentialité des codes dédiés au Service, par lui-même et par les Personnes habilitées.

Le Client est seul responsable vis-à-vis de la Banque du choix des Personnes habilitées et des opérations passées par ces dernières, notamment en cas de fraude ou d'abus de confiance. La Banque n'est tenue à cet égard à aucun contrôle ou vigilance particulière, et n'est pas tenue des conséquences financières qui résulteraient d'une mauvaise utilisation ou délivrance des codes susvisés.

15.2.2 - Responsabilité du Client sur les ordres saisis et déposés

Les ordres saisis ou déposés sont sous la responsabilité exclusive du Client. La Banque n'est tenue à cet égard à aucun contrôle ou vigilance particuliers. La Banque n'ayant pas d'autres contrôles à effectuer que le respect des habilitations indiquées dans les Conditions Particulières. A ce titre, la Banque n'est pas tenue responsable des conséquences financières qui résulteraient d'une mauvaise indication des montants et/ou des comptes de destinataires des ordres.

La Banque décline toute responsabilité pour les conséquences quelconques qui pourraient résulter des retards, des erreurs ou des omissions dans la transmission ou le contenu des messages adressés par le Client, ainsi que de leur mauvaise interprétation, pour autant que ces retards, erreurs, montages ou omissions ne soient pas imputables à la Banque.

15.3 - Cas d'une suppression de Personnes habilitées ou d'un changement de rôle

En cas de suppression d'une Personne habilitée ou d'un changement de rôle, le Client reste tenu des opérations effectuées par cette dernière et ce, antérieurement à la modification des Conditions Particulières.

15.4 - Cas particulier des opérations non autorisées consécutives à la perte ou au vol

Les parties conviennent expressément de déroger à l'article L.133-19 du code monétaire et financier de la façon suivante.

En cas d'opération de paiement non autorisée consécutive à la perte ou au vol d'un Instrument de Paiement et/ou de ses Données de sécurité personnalisées, il est précisé que :

- avant l'information prévue à l'article 6 ci-dessus, le payeur supporte toutes les pertes liées à l'utilisation de cet Instrument ou de ses Données de sécurité personnalisées. Toutefois, le Client ne supporte aucune conséquence financière :
  - en cas de perte ou de vol des Données de sécurité personnalisées ne pouvant être détectée par le Client avant le paiement du Client,
  - en cas de perte de ces Données de sécurité personnalisées due à des actes ou à une carence d'un salarié, agent ou d'une succursale de la Banque ou d'une entité vers laquelle ses activités ont été externalisées,
  - lorsque cette opération a été effectuée sans utilisation des Données de sécurité personnalisées,
  - lorsque l'opération non autorisée a été effectuée en détournant, à l'insu du Client, les Données de sécurité personnalisées liées à l'Instrument de paiement ou si elle résulte d'une contrefaçon de l'Instrument de paiement alors qu'au moment de l'opération de paiement non autorisée, il était en possession de son Instrument.
- à compter de l'information prévue à l'article 6, le payeur ne supporte aucune conséquence financière résultant de l'utilisation de l'Instrument de paiement ou de l'utilisation détournée des Données de sécurité personnalisées qui lui sont liées sauf agissement frauduleux de sa part. Dans le cadre d'une utilisation de Certificat électronique, cette disposition ne s'applique qu'à compter de la publication par l'Autorité de certification de la révocation du Certificat. Par conséquent, la Banque ne pourra pas être tenue responsable de la signature d'un ordre réalisée à l'aide d'un Certificat dont la révocation n'est pas encore publiée.

Le Client payeur supporte toutes les pertes occasionnées par des opérations de paiement non autorisées, si ces pertes résultent d'un agissement frauduleux de sa part ou s'il n'a pas satisfait, intentionnellement ou par négligence grave, aux obligations visées à l'article 6 ci-dessus.

Dans le cadre du présent contrat, l'indemnisation due par la partie responsable sera limitée aux seules pertes directes en capital et en trésorerie, subies par l'autre partie.

ARTICLE 16 - SECRET PROFESSIONNEL

La Banque est tenue au secret professionnel, conformément aux dispositions du Code monétaire et financier en vigueur.

Cependant, le secret est levé en vertu de dispositions légales, réglementaires, ou de conventions conclues par la France à des fins fiscales, notamment à l'égard de l'administration fiscale et des douanes, de la Banque de France, des organismes de sécurité sociale, de l'Autorité de contrôle prudentiel et de résolution, de l'autorité judiciaire agissant dans le cadre d'une procédure pénale, ainsi que dans le cadre d'une procédure civile, ou lorsqu'un texte spécifique le prévoit expressément.

La Banque peut partager avec les personnes, ci-après visées, avec lesquelles elle négocie, conclut ou exécute notamment les opérations, ci-après énoncées, des informations confidentielles concernant le Client, dès lors que ces informations sont nécessaires à celles-ci, ce que le Client accepte expressément :

- avec les entreprises qui assurent la mise en place ou la gestion d'un produit ou d'un service souscrit par le Client aux seules fins d'exécution des obligations contractuelles vis-à-vis de la Banque et du Client et plus généralement - avec des tiers (prestataires, sous-traitants, ...) en vue de leur confier des fonctions opérationnelles (par exemple : l'alerte sur l'utilisation de l'autorisation de découvert, le recours à des solutions de paiement mobile, la gestion des cartes bancaires, ou la fabrication de chéquiers) ;
- avec les entreprises qui assurent ou garantissent les crédits de ses clients (entreprises d'assurances, sociétés de caution mutuelle, par exemple) ;
- avec les entreprises qui octroient des crédits à ses clients ;
- avec des entreprises de recouvrement ;
- des entités appartenant au même groupe que la Banque (BPCE, Caisses d'Epargne, Oney Bank, BPCE Assurances, BPCE Financement, BPCE Lease et plus généralement toute autre entité du Groupe BPCE), pour l'étude ou l'élaboration de tous types de contrats ou d'opérations concernant ses clients ;
- des entreprises tierces en cas de cession de créances.

Les personnes recevant des informations couvertes par le secret professionnel, qui leur ont été fournies pour les besoins d'une des opérations ci-dessus énoncées, doivent les conserver confidentielles, que l'opération susvisée aboutisse ou non. Toutefois, dans l'hypothèse où l'opération susvisée aboutit, ces personnes peuvent à leur tour communiquer les informations couvertes par le secret professionnel.

Le Client victime d'une fraude ou d'une tentative de fraude autorise expressément la Banque à communiquer aux autorités policières et judiciaires son nom, son adresse, ainsi que son identifiant et plus généralement toute information nécessaire à la dénonciation de faits constitutifs d'un délit et ce afin d'apporter son concours à la justice dans le cadre de la lutte contre la fraude.

Il est précisé que les informations visées ci-dessus couvertes par le secret professionnel sont communiquées aux autorités judiciaires et policières dans le cadre étroit d'une enquête elle-même couverte par le secret visé à l'article 11 du Code de procédure pénale.

Le Client autorise expressément et dès à présent la Banque à communiquer et partager les données le concernant ainsi que leurs mises à jour :

- à BPCE S.A. agissant en qualité d'organe central du Groupe BPCE pour l'exercice des compétences prévues par le Code monétaire et financier afin que celui-ci puisse satisfaire aux différentes missions qui lui sont dévolues, au bénéfice de la Banque et du Groupe, notamment en matière de déclarations prudentielles auprès de toute autorité de régulation compétente ;
- à toute entité du Groupe BPCE en vue de la présentation au Client des produits ou services gérés par ces entités ;
- aux entités du Groupe BPCE avec lesquelles le Client est ou entre en relation contractuelle aux fins d'actualisation des données collectées par ces entités, y compris des informations relatives à son statut fiscal ;
- aux entités du Groupe BPCE en cas de mise en commun de moyens techniques, notamment informatiques ainsi que de gestion de gouvernance des données, pour le compte de la Banque. A cet effet, les informations personnelles concernant le Client couvertes par le secret bancaire pourront être pseudonymisées à des fins de recherches et de création de modèle statistique ;
- aux partenaires de la Banque, pour permettre au Client de bénéficier des avantages du partenariat auquel il adhère, le cas échéant, et ce dans le cadre exclusif des accords de partenariat ;
- aux sous-traitants et prestataires pour les seuls besoins des prestations à réaliser pour la Banque et notamment la fourniture des produits bancaires et financiers ou la réalisation d'enquêtes ou de statistiques.

Le Client autorise expressément la Banque à transmettre aux entités du Groupe BPCE auprès desquelles il a souscrit des produits ou services les informations actualisées sur son état civil, sa situation familiale, patrimoniale et financière, le fonctionnement de son compte ainsi que la note qui lui est attribuée pour l'application de la réglementation bancaire, afin de permettre l'étude de son dossier, l'utilisation des produits ou services souscrits, ou de leur recouvrement.

ARTICLE 17 - LUTTE CONTRE LE BLANCHIMENT DES CAPITAUX ET LE FINANCEMENT DU TERRORISME - RESPECT DES SANCTIONS INTERNATIONALES

17.1 - Lutte contre le blanchiment des capitaux et le financement du terrorisme

En application des dispositions légales et règlementaires prévues par le Code Monétaire et Financier (Livre V, Titre VI, Chapitre premier, partie législative et partie règlementaire), la Banque est tenue, dans le cadre de ses obligations relatives à la lutte contre le blanchiment des capitaux et le financement du terrorisme, de procéder à l'identification et à la vérification de l'identité des clients et le cas échéant, de leurs bénéficiaires effectifs. Un bénéficiaire effectif s'entend de la personne physique, soit qui contrôle, directement ou indirectement, une personne morale, soit pour laquelle une transaction est exécutée ou une activité réalisée.

Au même titre, la Banque est tenue de recueillir des informations relatives à l'objet et à la nature de la relation d'affaires, d'actualiser ces informations et d'exercer une vigilance constante à l'égard des opérations réalisées par sa clientèle pendant toute la durée de la relation d'affaires (montant et nature des opérations, provenance et destination des fonds, suivi de la situation professionnelle, économique et financière du Client ...).

A cette fin, le Client s'engage à fournir, à première demande, à la Banque ces informations et les justificatifs afférents. A défaut de les fournir ou en cas de fourniture d'informations erronées par le Client, la Banque pourra être conduite, en vertu des dispositions légales et réglementaires précitées, à résilier les conventions conclues avec le Client.

La Banque est également tenue d''appliquer des mesures de vigilance complémentaires à l''égard de ses clients Personnes Politiquement Exposées (P.P.E.) définies aux articles L. 561-10 1° et R. 561-18 du Code Monétaire et Financier, et par les dispositions de l''arrêté ministériel du 17 mars 2023 fixant en application dudit article R. 561-18 la liste des fonctions françaises concernées, ou à l'égard de ses clients personnes morales dont les bénéficiaires effectifs seraient dans cette situation. A ce titre, la Banque peut procéder, selon le cas, à un recueil d'informations auprès du Client et/ou auprès de sources externes.

Par ailleurs, le Client s'engage à fournir, à première demande, à la Banque, toute information et justificatif nécessaire, en cas d'opération(s) qui apparaîtrait(ont) à la Banque comme particulièrement complexe(s) ou d'un montant inhabituellement élevé ou dépourvue(s) de justification économique ou d'objet licite. A défaut de les fournir ou en cas de fourniture d'informations erronées par le Client, celui-ci est informé que la Banque se réserve la possibilité de ne pas exécuter l'opération ou de mettre un terme à l'opération et qu'elle pourra être conduite, en vertu des dispositions légales et réglementaires précitées, à résilier les conventions conclues avec le Client.

Le Client est informé que la Banque est tenue de déclarer les sommes inscrites dans ses livres et les opérations portant sur des sommes qui pourraient provenir d'une infraction passible d'une peine privative de liberté supérieure à un (1) an, ou qui pourraient être liées au financement du terrorisme. Ces obligations portent également sur les tentatives d'opérations. Ladite déclaration à la Cellule de Renseignement Financier est réalisée en application des dispositions des articles L. 561-15 et L. 561-18 du Code Monétaire et Financier.

Le Client est informé que les pouvoirs publics peuvent exiger de la Banque qu'elle n'exécute pas une opération demandée ou initiée par le Client, en application des dispositions de l'article L. 561-24 du Code Monétaire et Financier.

Pour la mise en œuvre de ces obligations et pendant toute la durée du Contrat, le Client s'engage envers la Banque :

- à respecter l'ensemble des obligations légales et règlementaires nationales relatives à la lutte contre le blanchiment d'argent et le financement du terrorisme ainsi que les législations étrangères équivalentes, dans la mesure où celles-ci sont applicables ;
- à ne pas utiliser, prêter, investir ou apporter ses fonds dans des opérations qui contreviendraient aux obligations de lutte contre le blanchiment de capitaux et le financement du terrorisme précitées ;
- à la tenir informée, sans délai, de toute modification survenue au niveau de ses situations personnelle, professionnelle, patrimoniale, financière ou de celles de sa caution éventuelle, et plus généralement de tout événement susceptible de modifier notoirement la valeur de son patrimoine ou d'aggraver l'importance de son endettement, ainsi que de toute modification relative à ses représentants légaux, actionnaires ou bénéficiaires effectifs ;
- à lui communiquer, à sa demande et sans délai, toute information, toute pièce ou tout document relatif à sa situation personnelle, professionnelle, patrimoniale ou financière ou aux conditions d'une opération inhabituelle initiée à son profit ou au profit d'un tiers.

Le Client est informé que la Banque est tenue de conserver, pendant cinq (5) ans à compter de la résiliation des conventions conclues avec le Client, l'ensemble des informations et documents le concernant, sans préjudice de l'obligation de conservation d'informations et documents le concernant pour d'autres produits et services fournis par la Banque, en application des dispositions de l'article L. 561-12 du Code Monétaire et Financier.

17.2 - Respect des sanctions internationales

La Banque est tenue de respecter les lois et réglementations en vigueur dans diverses juridictions, en matière de sanctions

économiques, financières ou commerciales, et de respecter toute mesure restrictive liée à un embargo, à un gel des avoirs et des ressources économiques, à des restrictions sur des transactions avec des individus ou entités ou concernant des biens ou des territoires déterminés émises, administrées ou mises en place par le Conseil de sécurité de l'ONU, l'Union européenne, la France, les États-Unis d'Amérique (et notamment le Bureau de Contrôle des Actifs Etrangers rattaché au Département du Trésor : OFAC et le Département d'État) et par des autorités locales compétentes pour édicter de telles sanctions (ci-après les « Sanctions Internationales »).

Dans le cas où le Client, son mandataire éventuel, le bénéficiaire effectif, une contrepartie du Client, ou l'Etat dans lequel ils résident viendraient à faire l'objet de telles sanctions ou mesures restrictives, le compte du Client serait utilisé en violation des Sanctions Internationales, notamment pour recevoir ou transférer, de façon directe ou indirecte, des fonds en provenance ou à destination d'une contrepartie soumise directement ou indirectement aux Sanctions Internationales ou localisée dans un pays sous sanctions, la Banque pourra être amenée, en conformité avec celles-ci, à suspendre ou rejeter une opération de paiement ou de transfert émise et/ou reçue par le Client, qui pourrait être ou qui, selon son analyse, serait susceptible d'être sanctionnée par toute autorité compétente, ou le cas échéant, à bloquer les fonds et les comptes du Client ou à résilier le Contrat.

A ce titre, le Client déclare :
- Qu'il n'est pas une personne qui fait l'objet ou est la cible de Sanctions Internationales, ci-après une « Personne Sanctionnée » ;
- Qu'il n'est pas une personne située, constituée ou résident d'un pays ou un territoire qui fait, ou dont le gouvernement fait, l'objet d'un régime de Sanctions Internationales interdisant ou restreignant les relations avec ledit gouvernement, pays ou territoire ci-après un « Pays Sanctionné » ;
- Qu'il n'est pas une personne engagée dans une activité avec une Personne Sanctionnée ;
- Qu'il n'est pas une personne ayant reçu des fonds ou tout autre actif ou envoyé des fonds en provenance ou à destination d'une Personne Sanctionnée ;
- Qu'il n'est pas une personne engagée dans une activité avec une personne située, constituée ou résident d'un Pays Sanctionné.

Le Client s'engage envers la Banque, pendant toute la durée du Contrat :
- à informer sans délai la Banque de tout fait dont il aura connaissance qui viendrait rendre inexacte l'une ou l'autre des déclarations relatives aux Sanctions Internationales ;
- à ne pas utiliser directement ou indirectement ses fonds et à ne pas prêter, apporter ou rendre autrement disponible ses fonds à toute autre personne pour toute opération qui aurait pour objet ou effet le financement ou la facilitation des activités et des relations d'affaires avec une Personne Sanctionnée ou située, constituée ou résidente dans un Pays Sanctionné ou susceptibles de constituer une violation des Sanctions Internationales ;
- à n'utiliser aucun revenu, fonds ou profit provenant de toute activité ou pération réalisée avec une Personne Sanctionnée ou avec toute personne située, constituée ou résident d'un Pays Sanctionné dans le but de rembourser ou payer les sommes dues à la Banque au titre du présent contrat ;
- à la tenir informée sans délai de toute modification survenue au niveau de ses situations professionnelle, patrimoniale, financière ou personnelle ou de celles de sa caution éventuelle, et plus généralement de tout événement susceptible de modifier notoirement la valeur de son patrimoine ou d'aggraver l'importance de son endettement.

A défaut, la Banque se réserve la possibilité de ne pas exécuter l'opération ou de mettre un terme à l'opération.

ARTICLE 18 - LUTTE CONTRE LA CORRUPTION ET LE TRAFIC D'INFLUENCE

La Banque est tenue, dans le cadre de ses obligations légales et règlementaires (en particulier issues de la loi n° 2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique) concernant la lutte contre les atteintes à la probité, dont la corruption et le trafic d'influence, de procéder à l'évaluation de l'intégrité de sa clientèle pendant toute la durée de la relation d'affaires, au regard de critères de risques tels que :
- les bénéficiaires effectifs ;
- les pays de résidence et d'activité ;
- les secteurs d'activité ;
- la réputation et ;
- la nature, et l'objet de la relation ;
- les autres intervenants (écosystème) ;
- les interactions avec des agents publics ou des Personnes Politiquement Exposées (P.P.E) définies aux articles L. 561-10 1° et R. 561-18 du Code Monétaire et Financier et par les dispositions de l'arrêté ministériel du 17 mars 2023 fixant en application dudit article R. 561-18, la liste des fonctions françaises concernées ;
- les aspects financiers en jeu et devises traitées.

Le Client s'engage en conséquence :
- à permettre à la Banque de satisfaire aux obligations légales mentionnées ci-dessus visées, notamment en lui apportant toutes les informations nécessaires, spontanément ou à la demande de la Banque ;
- à ne pas effectuer sur ses comptes ouverts dans les livres de la Banque, d'opération(s) visant ou liée(s) à la commission d'un fait de corruption ou de trafic d'influence, de concussion, de prise illégale d'intérêt, de détournement de fonds publics ou de favoritisme, et à justifier sur demande les opérations sans objet apparent ;
- à ne pas proposer ou offrir de cadeaux, invitations ou autres avantages à un salarié de la Banque afin d'obtenir un avantage indu relatif au fonctionnement de ses comptes ouverts dans les livres de la Banque.

ARTICLE 19 - PROTECTION DES DONNÉES PERSONNELLES

Dans le cadre de la signature et de l'exécution du Contrat, la Banque recueille et traite des données à caractère personnel concernant les personnes physiques intervenant dans le cadre de ce Contrat (mandataire, représentant légal, caution, contact désigné, préposé, bénéficiaire effectif...).

Les informations expliquant pourquoi et comment ces données sont utilisées, combien de temps elles seront conservées ainsi que les droits dont ces personnes disposent sur leurs données figurent dans la Notice d'information de la Banque sur le traitement des données à caractère personnel. Cette notice est disponible à tout moment sur le site internet de la Banque via l'adresse suivante : https://www.caisse-epargne.fr/ile-de-france/protection-donnees-personnelles ou sur simple demande auprès de l'agence du Client. La Banque communiquera en temps utile les évolutions apportées à ces informations.

ARTICLE 20 - DURÉE ET RÉSILIATION

20.1 - Durée du contrat

Le Contrat prend effet à compter du jour de sa signature. Il est conclu pour une durée indéterminée.

20.2 - Résiliation sans motif

Chacune des parties peut mettre fin au présent contrat, par écrit (auprès de son agence ou par lettre recommandée avec demande d'avis de réception), à tout moment, sans avoir à indiquer ni justifier du motif.

Lorsqu'elle est effectuée par le Client, la résiliation devient effective au terme d'un délai de trente (30) jours à compter de la réception par la Banque de l'écrit adressé par le Client.

La résiliation par la Banque doit respecter un préavis de trente (30) jours.

Sauf indication contraire du Client, la résiliation de l'une des prestations optionnelles de CE net n'entraîne la résiliation que de cette seule prestation, l'abonnement de CE net continuant de produire ses effets entre les parties.

20.3 - Résiliation pour manquement

En cas de manquement par l'une quelconque des parties aux obligations dont elle a la charge au titre du Contrat, et auquel il n'aurait pas été remédié dans un délai de huit (8) jours à compter de l'envoi d'une lettre recommandée avec demande d'avis de réception, l'autre partie pourra, prononcer la résiliation de la Convention.

20.4 - Résiliation de plein droit

La résiliation de la convention de compte courant entraîne la résiliation automatique du Contrat.

20.5 - Effets de la résiliation

En cas de cessation de la Convention, pour quelque motif que ce soit, les Parties sont tenues de prendre toutes dispositions utiles en vue du dénouement des opérations en cours. Tout ordre donné avant la date effective de résiliation est exécuté aux conditions et dates convenues.

La résiliation du Contrat entraîne de plein droit la résiliation du service de Signature électronique et/ou d'Authentification forte sur CE net liés au Contrat.

20.6 - Possibilité de suspension par la Banque

La Banque se réserve le droit de bloquer sans délai, sans aucun préavis, ni formalité, le service CE net, ou une Personne habilitée, pour des raisons objectivement motivées liées à la sécurité du Service, à la présomption d'une utilisation non autorisée ou frauduleuse du Service ou au risque sensiblement accru ou avéré que le Client soit dans l'incapacité de s'acquitter de son obligation de paiement. Dans ces cas, la Banque informe le Client, par tous moyens, du blocage et des raisons de ce blocage, si possible avant que le Service ne soit bloqué ou immédiatement après sauf si cette information est impossible pour des raisons de sécurité ou interdite par une législation communautaire ou nationale. La Banque débloque le Service dès lors que les raisons du blocage n'existent plus.

ARTICLE 21 - RÉCLAMATIONS - MÉDIATION

En cas de difficultés concernant ces produits et services, le Client peut obtenir de son Agence toutes les informations souhaitées, formuler auprès d'elle toute réclamation et/ou saisir par écrit le « Service Relations Clientèle » de la Banque qui s'efforce de trouver avec lui une solution, y compris si la réponse ou solution qui lui a été apportée par son Agence ne lui convient pas.

Le Client trouvera les coordonnées du service en charge des réclamations dans les brochures tarifaires de la Banque ainsi que sur son site internet, dans la rubrique « Contact » ou en saisissant « Réclamation » dans le moteur de recherche.

- Pour la clientèle des Entreprises et Institutionnels, la saisine du Service Clients BDR est effectuée par courrier adressé à l'adresse suivante : Caisse d'Epargne Ile-de-France - Service Clients BDR - 26/28, rue Neuve Tolbiac - CS 91344 - 75633 Paris Cedex 13.
- Pour la clientèle des Professionnels et Associations, la saisine du Service Relations Clientèle est effectuée par courrier adressé à l'adresse suivante: Caisse d'Epargne Ile-de-France - Service Relations Clientèle - 26/28, rue Neuve Tolbiac - CS 91344 - 75633 Paris Cedex 13.

La Banque s'engage à accuser réception de la réclamation du Client sous dix (10) Jours Ouvrables à compter de sa date d'envoi, sauf si une réponse peut être apportée dans ce délai. Si une analyse plus approfondie de son dossier est nécessaire, la Banque s'engage à lui apporter une réponse dans un délai qui ne pourra excéder deux (2) mois (à compter de la date d'envoi de sa réclamation).

Concernant les réclamations liées aux services de paiement, une réponse sera apportée au Client dans les quinze (15) Jours Ouvrables suivant la réception de sa réclamation. Cependant, si un délai supplémentaire est nécessaire pour lui répondre, la Banque lui adressera une réponse d'attente motivant ce délai et précisant la date ultime de sa réponse. En tout état de cause, le Client recevra une réponse définitive au plus tard trente-cinq (35) Jours Ouvrables suivant la réception de sa réclamation.

A défaut de solution le satisfaisant ou en l'absence de réponse dans ces délais, le Client, dès lors qu'il est un Entrepreneur individuel au sens de l'article L. 526-22 du Code de Commerce et uniquement dans ce cas, a la faculté de saisir gratuitement le médiateur de la Banque sur son site internet ou par voie postale, dans le délai d'un (1) an à compter de sa réclamation auprès de la Banque, sans préjudice des autres voies d'actions légales dont il dispose.

L'adresse postale du médiateur et les coordonnées du site internet du médiateur figurent sur les brochures tarifaires et le site internet de la Banque.

Les informations nécessaires à la saisine du médiateur, son périmètre et le déroulé de la procédure de médiation figurent sur la charte de médiation disponible sur le site internet du médiateur.

ARTICLE 22 - DROIT ET LANGUE APPLICABLES

22.1 - Élection de domicile

Pour l'exécution du Contrat, il est fait élection de domicile par la Banque, en son siège social ou au lieu de son établissement principal, par le Client, au lieu d'exercice de son activité, à son adresse ou à son siège social indiqué aux Conditions Particulières.

22.2 - Langue et droit applicables - Attribution de compétence

Le Contrat est conclu en langue française. Le Client accepte expressément l'usage de la langue française durant les relations contractuelles et précontractuelles.

Le Contrat est soumis au droit français.

En cas de contestation, pour quelque cause que ce soit, la Banque et le Client porteront tout litige auprès du Tribunal compétent dans le ressort duquel est situé le siège social de la Banque. Cette stipulation n'est applicable que si le Client a la qualité de commerçant.

ARTICLE 23 - DOCUMENTS CONTRACTUELS

Les documents contractuels applicables par ordre de préséance sont :

- De manière égale, les Conditions Particulières, comprenant en annexe les synthèses des habilitations, la synthèse des délégations des signatures et la synthèse du Collège de signature,
- Les présentes Conditions Générales,
- La Convention de compte courant,
- Les contrats liés aux différents protocoles utilisés (EBICS, SWIFTNET),
- Les autres contrats négociés par ailleurs entre les Parties.

CAISSE D'EPARGNE
Ile de France

CE net - Conditions générales

en vigueur à compter du 1er décembre 2026

SOMMAIRE

PRÉAMBULE 2

DÉFINITIONS 2

ARTICLE 1 - OBJET 4

ARTICLE 2 - PRINCIPAUX SERVICES DISPONIBLES DANS CE NET 4

ARTICLE 3 - PERSONNES HABILITÉES À UTILISER LE SERVICE 15

ARTICLE 4 - MOYENS MATÉRIELS ET TECHNIQUES D'ACCÈS À CE NET 17

ARTICLE 5 - CONDITIONS D'ACCÈS ET DE SÉCURITÉ DE CE NET 17

ARTICLE 6 - OPPOSITION À L'UTILISATION DES SERVICES EN LIGNE CE NET 22

ARTICLE 7 - CONDITIONS D'EXÉCUTION DES OPÉRATIONS ET ORDRES DE PAIEMENT DÉPOSÉS VIA CE NET, TRANSMIS VIA UN TIERS INITIATEUR DE PAIEMENT (API), OU TRANSMIS VIA UN PROTOCOLE DE COMMUNICATION BANCAIRES EDI 23

ARTICLE 8 - MODALITÉS D'AUTORISATION DES ORDRES DE PAIEMENT 25

ARTICLE 9 - MODALITÉ DE CONFIRMATION DES FICHIERS DE REMISES D'ORDRES DÉPOSÉS VIA LE SERVICE OU TRANSMIS PAR UN PROTOCOLE DE COMMUNICATION BANCAIRE 26

ARTICLE 10 - CONDITIONS D'UTILISATION ET DISPONIBILITÉ DU SERVICE 26

ARTICLE 11 - PREUVE DES OPÉRATIONS ET DÉLAI DE RÉCLAMATION 27

ARTICLE 12 - INTÉGRITÉ, CONFIDENTIALITÉ DU SERVICE 27

ARTICLE 13 - MODIFICATION DES CONDITIONS PARTICULIÈRES ET DES CONDITIONS GÉNÉRALES DE CE NET 27

ARTICLE 14 - TARIFICATION 28

ARTICLE 15 - RESPONSABILITÉS DE LA BANQUE ET DU CLIENT 28

ARTICLE 16 - SECRET PROFESSIONNEL 30

ARTICLE 17 - LUTTE CONTRE LE BLANCHIMENT DES CAPITAUX ET LE FINANCEMENT DU TERRORISME - RESPECT DES SANCTIONS INTERNATIONALES 31

ARTICLE 18 - LUTTE CONTRE LA CORRUPTION ET LE TRAFIC D'INFLUENCE 32

ARTICLE 19 - PROTECTION DES DONNÉES PERSONNELLES 33

ARTICLE 20 - DURÉE ET RÉSILIATION 33

ARTICLE 21 - RÉCLAMATIONS - MÉDIATION 34

ARTICLE 22 - LANGUE ET DROIT APPLICABLES - ATTRIBUTION DE COMPÉTENCE 34

ARTICLE 23 - ÉLECTION DE DOMICILE 34

ARTICLE 24 - DOCUMENTS CONTRACTUELS 34

Mod. 07.00.000765 - 07/2026 - DJ CONSEIL : 07/2026 - Page 1/34

PRÉAMBULE

Le présent contrat relatif au Service de Banque à distance CE net (ci-après le « Contrat ») se compose des Conditions Particulières, des présentes Conditions Générales, des Conditions Tarifaires ainsi que de ses éventuelles annexes et avenants. Le Contrat est complété par la convention de compte courant et toutes autres conventions existantes liées à des services spécifiques signées par le Client, par acte séparé, ainsi que le cas échéant par les conventions/contrats liés aux différents protocoles utilisés par le Client (EBICS, SWIFTNET).

Les opérations effectuées dans le cadre du Service ne sauraient déroger aux Conditions Particulières et/ou Générales d'autres produits ou services ouverts ou à ouvrir, sauf stipulation contraire.

DÉFINITIONS

Abonné ou Client : personne physique agissant à des fins professionnelles, ou personne morale ayant souscrit ou utilisant le Service CE net et titulaire d'un compte courant dans les livres de la Banque.

Administrateur(s) : la ou ou les personnes physiques, désignée(s) aux Conditions Particulières du Contrat par le Client, qui a (ont) en charge la gestion des droits des Utilisateurs dans la limite du périmètre de l'abonnement (comptes, Services, Utilisateurs) indiqué aux Conditions Particulières.

Application mobile : Programme téléchargeable de façon gratuite et exécutable à partir du système d'exploitation d'un smartphone ou d'une tablette, permettant aux Personnes habilitées d'utiliser le Service, dans le périmètre et les limites de leurs habilitations respectives.

Authentification : Procédure qui permet de vérifier l'identité d'une Personne habilitée ou la validité de l'utilisation de l'Instrument de paiement, y compris l'utilisation des données de sécurité personnalisées de cette personne.

Authentification forte : procédure d'Authentification reposant sur l'utilisation d'au moins deux éléments parmi les trois catégories suivantes : 1) une information que la Personne habilitée est seule à connaître (mot de passe, code secret, code PIN), 2) l'utilisation d'un appareil qui appartient à la Personne habilitée (téléphone portable, montre connectée, appareil dédié fourni par la Banque...), 3) une caractéristique personnelle qui est intimement liée à la Personne habilitée (empreinte digitale, reconnaissance faciale, vocale...).

Banque : désigne la Caisse d'Epargne fournissant le Service.

CE net : désigne le service de Banque à distance fourni par la Banque à des fins d'utilisation professionnelle.

Certificat électronique : Document électronique attestant du lien entre les données de vérification de Signature électronique et un signataire.

CFONB : Comité Français d'Organisation et de Normalisation Bancaires.

Compte donneur d'ordre : compte à partir duquel l'opération est initiée par le donneur d'ordre.

Collège de signature : Regroupement d'Utilisateurs détenant une délégation de signature des remises d'ordre pour valider un même périmètre d'opérations définies aux Conditions Particulières. Le Service permet de paramétrer les droits de signature de l'abonnement CE net au niveau d'un groupe d'Utilisateurs signataires qui forment alors un Collège de signature.

Compte destinataire : compte vers lequel l'opération est initiée par le donneur d'ordre.

Digital Box : Ce service permet au Client de bénéficier de la mise à disposition, en format électronique, de certains documents lis à la gestion d'un produit bancaire. Les conditions générales d'utilisation de Digital Box complètent les présentes conditions générales.

Digital Share : Service d'échange de documents entre le Client et la Banque.

Données de sécurité personnalisées : données confidentielles fournies par la Banque à un Client ou un Abonné pour l'utilisation d'un Instrument de paiement. Ces données, propres au Client et placées sous sa garde, visent à l'authentifier et à sécuriser ses opérations dans le cadre de CE net.

EDI : Echanges de Données Informatisées ou Electronic Data Interchange peut être défini comme l'échange, d'ordinateur à ordinateur, d'entreprises à établissements bancaires, de données concernant des transactions en utilisant des réseaux de télécommunication et des formats normalisés, directement exploitables par leurs systèmes d'informations. L'EDI peut se faire selon différents protocoles, dont notamment le protocole EBICS. Pour bénéficier du service EDI, le Client doit conclure avec la Banque le contrat relatif à l'EDI et/ou le contrat relatif au protocole d'échange retenu, tel le protocole EBICS.

EBICS : Electronic Banking Internet Communication Standard. Protocole multi-bancaire utilisé sur Internet avec un haut niveau de sécurité permettant une Authentification réciproque par Certificats. Deux modes d'utilisation d'EBICS se distinguent dans le sens Client vers Banque : EBICS profil T (transport) et EBICS profil TS (Transport et Signature). Le Client doit s'équiper d'un logiciel de communication EBICS T ou EBICS TS pour pouvoir utiliser le protocole EBICS. EBICS permet des échanges de fichiers volumineux.

EBICS profil T : Les fichiers envoyés par le Client à la Banque ne sont pas accompagnés de la ou des signature(s) personnelle(s) jointe(s). Les données envoyées ne pourront être prises en compte que si la Banque se trouve en possession d'un ordre de validation transmis par un autre canal.

EBICS profil TS : Les fichiers envoyés par le Client à la Banque sont accompagnés dans la même transmission de la ou des signature(s) personnelle(s) jointe(s) prévue(s) pour l'échange des données concernées.

Espace de Banque à distance : espace sécurisé propre au Client, accessible par internet depuis le Site ou depuis l'Application mobile de la Banque où le Service est disponible.

Instrument de paiement : dispositif personnalisé et/ou un ensemble de procédures convenu entre le Client et la Banque utilisé(s) pour donner un ordre de paiement.

Jour Ouvrable : désigne un jour au cours duquel la Banque ou la banque du bénéficiaire ainsi que tous les autres intervenants à l'exécution d'une opération de paiement exercent une activité permettant d'exécuter celle-ci.

Lecteur CAP : appareil lecteur de carte à puce fourni par la Banque à l'Utilisateur du service SOL par lecteur CAP (Sécurisation des Opérations en Ligne). Il nécessite l'utilisation d'une carte business ou d'une carte Secur@ccès afin de fournir un code de contrôle.

Messagerie Sécurisée Internet (MSI) : Dans le cadre de l'abonnement à CE net, le Client et les Utilisateurs ont accès à une messagerie électronique dans l'environnement sécurisé de CE net, dénommée la « Messagerie Sécurisée Internet » (ci-après « MSI »), dont les Conditions Générales d'Utilisation figurent à l'article 2.3.2.6 ci-après.

Opérations sensibles : opérations de Banque à distance nécessitant une Authentification forte afin de prévenir le risque de fraude.

Personnes habilitées : désigne l'Utilisateur Principal, les Administrateurs et les Utilisateurs autorisés à agir au nom et pour le compte du Client.

Parafeur : Espace dédié à la Signature électronique des remises d'ordres.

Pare-feu (firewall) : Dispositif qui protège un système informatique connecté à Internet des tentatives d'intrusion.

Référentiel : ensemble des Comptes destinataires de l'abonnement CE net du Client.

Relevés d'opérations : relevés détaillés des opérations reçues, rejets sur des opérations émises.

Services : Ensemble des fonctionnalités de CE net.

Services CE net « aller » : Echanges de Données Informatisées du Client vers la Banque.

Services CE net « retour » : Echanges de Données Informatisées de la Banque vers le Client.

Site : désigne le site Internet permettant l'accès aux Services de CE net.

Signature électronique : Signature utilisant un procédé électronique fiable d'Identification de son auteur et garantissant son lien avec l'acte auquel elle s'attache.

Synthèse des comptes : La Synthèse des comptes permet au Client d'avoir une vision globale du solde de chacun de ses comptes.

Transporteur de données : « Utilisateur » technique qui transfère et réceptionne les flux via un logiciel de communication bancaire. Il ne peut pas avoir de droit de signature bancaire sur les flux. Il est compatible avec les protocoles EBICS, Swift Net (FileAct et FIN).

TurboSign : Extension du navigateur internet qui permet de faire dialoguer CE net depuis un navigateur Chrome ou Firefox avec le Certificat électronique. L'installation de cette extension est proposée à l'utilisateur à la première utilisation du Certificat dans CE net. Cette extension est à installer sur chaque poste de travail sur lequel le Certificat électronique sera utilisé.

Utilisateur Principal : personne physique, désignée aux Conditions Particulières du Contrat qui peut utiliser le Service, dans l'ensemble du périmètre de l'abonnement indiqué aux Conditions Particulières, et qui a également le profil d'Administrateur dans les limites des fonctions accessibles en ligne.

Utilisateur(s) : la ou les personnes, désignée(s) aux Conditions Particulières du présent contrat, habilitée(s) à utiliser le Service, dans le périmètre qui lui (leur) a été imparti par le ou les Administrateurs et le cas échéant par l'Utilisateur Principal, et dans les limites des fonctions accessibles en ligne.

ARTICLE 1 - OBJET

Le Contrat détermine les conditions d'accès et d'utilisation du Service de Banque à Distance CE net fourni par la Banque. Ce Service permet au Client par l'intermédiaire des Personnes habilitées, d'effectuer des opérations à distance selon les options retenues :

- la consultation de son ou ses comptes, l'obtention de divers renseignements liés à différents produits qu'il détient, la réalisation d'opérations portant sur son ou ses comptes (saisie d'ordres de paiement, gestion et suivi des ordres en ligne, ...), la possibilité de souscrire à des contrats et services complémentaires (sous réserve d'être préalablement habilité à souscrire le contrat ou service et à engager le Client).
- les Echanges de Données Informatisées (EDI), la saisie d'opérations, la gestion et le suivi des ordres en ligne, ainsi qu'un service de Signature électronique. Pour ce faire, la Banque met à la disposition du Client :
  - des protocoles de communication bancaire tels que EBICS, SWIFTNet, FileAct ou SWIFTNet FIN permettant l'EDI dans les deux sens de la relation (Client/banque : émission d'ordres & banque/Client : réception de relevés...) et des services associés sur le serveur EDI de la Banque,
  - un Site sécurisé permettant le dépôt de remises d'ordres, la récupération de relevés et des services associés.

Le Service est disponible depuis l'Espace de Banque à distance du Client. Certains services/fonctionnalités sont disponibles uniquement via le Site ou via l'Application mobile.

Le Client souscrit à tout ou partie du Service dans les Conditions Particulières du Contrat.

Le Client s'engage à remettre à l'ensemble des Personnes habilitées à utiliser CE net, un exemplaire des présentes Conditions Générales ainsi que les conditions générales de la convention de compte courant, et de toutes leurs modifications à venir.

La Banque se réserve le droit de modifier le contenu du Service et/ou de l'une ou de l'ensemble des fonctionnalités du Service notamment en vue d'en améliorer la qualité ou par l'adjonction de nouvelles fonctionnalités. Le cas échéant, le Client sera informé des éventuels impacts contractuels et tarifaires dans les conditions prévues à l'article 13 du Contrat.

ARTICLE 2 - PRINCIPAUX SERVICES DISPONIBLES DANS CE NET

Le Client désigne aux Conditions Particulières du Contrat lors de la souscription la liste des comptes concernés par l'abonnement, les services auxquels il souhaite souscrire, les types d'opération et, le cas échéant, les formats de fichiers associés, ainsi que les Personnes habilitées à utiliser le Service.

Toute modification de ces choix donnera lieu à la signature d'avenants aux Conditions Particulières sauf, sous réserve de disponibilité, si cette modification résulte d'un choix du Client effectué directement par ce dernier sur son Espace de Banque à Distance.

CE net se décline en cinq offres en fonction des besoins du Client : CE net Initial, CE net Confort, CE net Comptes, CE net Remises et CE net EDI. Une offre spécifique CE net COPRO peut également être proposée par la Banque.

Le périmètre exact des fonctionnalités accessibles au Client dépend de l'offre et des restrictions qui lui sont applicables au titre du présent article.

2.1 - CE net Initial

Sous réserve de disponibilité, CE net Initial permet au Client d'effectuer les opérations décrites à l'article 2.3 (CE net Comptes) sous les restrictions cumulatives suivantes :

- Gestion des Personnes Habilitées : CE net Initial est limité à la désignation d'un unique Utilisateur Principal au sens de l'article 3.1. Les fonctionnalités de création et de gestion d'Administrateurs et d'Utilisateurs supplémentaires mentionnées aux articles 3.2 et 3.3 ne sont pas disponibles. En conséquence, les dispositions des présentes Conditions Générales relatives aux Personnes Habilitées doivent être comprises et interprétées en tenant compte de cette limitation au seul Utilisateur Principal. Les stipulations de l'article 3 ne s'appliquent à CE net Initial que dans la limite de ce qui est compatible avec l'absence d'Administrateur et d'Utilisateur supplémentaire.
- Périmètre des virements : Le Client ne peut initier que des ordres de virement SEPA unitaires. Les fonctionnalités de virements groupés décrites à l'article 2.3.2.2 ne sont pas disponibles. Le Client ne peut pas réaliser de virements internationaux ou de virements de trésorerie.

CE net Initial prend la dénomination commerciale de CE net Reddy lorsque le Client, entrepreneur individuel ou société unipersonnelle, a souscrit à l'offre groupée de services Reddy, dont il est une composante.

Sous réserve de disponibilité, CE net Reddy comporte les mêmes fonctionnalités que celles de CE net Initial à l'exception des spécificités suivantes :

- l'Espace de Banque à distance est accessible depuis l'application mobile Reddy ou depuis le site Internet Reddy dont l'adresse URL est communiquée au Client par la Banque,
- les fonctionnalités relatives aux chèques, aux opérations de financement et à la Messagerie Sécurisée Internet décrites respectivement aux articles 2.3.2.3, 2.3.2.5 et 2.3.2.6 des Conditions Générales ne sont pas disponibles,
- compte tenu des spécificités de l'offre groupée de services Reddy, le Client ne dispose pas d'une gestion en agence et n'a pas accès à un conseiller dédié. Les demandes d'assistance peuvent être adressées par le Client via la rubrique « Contact » de son Espace de banque à distance Reddy ou via la rubrique « Nous contacter » depuis le site Internet Reddy. Sans préjudice des stipulations de l'article « Réclamations - Médiation » des Conditions Générales, le Client peut également déposer une réclamation via la rubrique « Nous contacter » du site Internet Reddy.

En cas de résiliation de l'offre groupée de services Reddy, le Service de banque à distance du Client se poursuit dans le cadre de CE net Initial, sauf résiliation concomitante de celui-ci. Il est alors régi par les dispositions des Conditions Générales et par les conditions tarifaires applicables à CE net Initial.

2.2 - CE net Confort

Sous réserve de disponibilité, CE net Confort permet au Client d'effectuer les opérations décrites à l'article 2.3 (CE net Comptes) sous la restriction suivante :

- Périmètre des virements : Le Client ne peut initier que des ordres de virement SEPA unitaires. Les fonctionnalités de virements groupés décrites à l'article 2.3.2.2 ne sont pas disponibles. Le Client ne peut pas réaliser de virements internationaux ou de virements de trésorerie.

2.3 - CE net Comptes

CE net Comptes permet au Client d'effectuer par l'intermédiaire des Personnes habilitées à utiliser le Service, les principales opérations décrites ci-après (la liste n'étant pas exhaustive).

2.3.1 - Gestion des accès à CE net Comptes

L'accès des Utilisateurs à CE net Comptes est paramétré à la fois lors de la souscription par le Client dans les Conditions Particulières mais aussi via son Espace de Banque à distance à partir de l'onglet « Paramétrage », en cliquant sur « Gestion des utilisateurs ».

2.3.2 - Principaux Services disponibles dans CE net Comptes

2.3.2.1 - Consultation

- <u>CONSULTATION DES COMPTES ET DES OPÉRATIONS</u>
  Le Client peut consulter la position du ou de ses comptes (en date comptable ou en date de valeur), compris dans le périmètre du Service, les dernières opérations de débit et/ou de crédit intervenues sur le ou les comptes, sous réserve qu'elles ne remontent pas à plus de cent quatre-vingts jours (180) jours, ainsi que les débits en instance de la/des carte(s) bancaire(s) s'il y a lieu.

  Le Client peut consulter les opérations à venir, ainsi que le solde prévisionnel de son ou de ses comptes courant(s) sur les sept (7) jours à venir. Ces informations sont communiquées à titre indicatif, seules les écritures mentionnées sur le relevé de compte ou l'arrêté de compte faisant foi entre les parties.

  Il est possible de télécharger le détail des opérations.

- <u>CONSULTATION DE L'ACTIVITE MONÉTIQUE</u>
  Le Client peut consulter certains de ses contrats monétiques, ainsi que ses locations de matériel (terminal de paiement électronique) souscrits auprès de la Banque. Il peut également consulter via un tableau de bord, l'ensemble de son activité monétique.

- <u>CONSULTATION ET GESTION DES MANDATS DE PRÉLÈVEMENT SEPA ET DES OPÉRATIONS DE PRÉLÈVEMENTS REÇUS AU DÉBIT DU COMPTE</u>
  Le Client a la possibilité de consulter les mandats de prélèvements SEPA CORE, les prélèvements exécutés et à venir, de bloquer et réactiver les prélèvements et de gérer les mandats de prélèvements SEPA interentreprises reçus en attente d'être débités sur son compte ou déjà débités.

- <u>CONSULTATION ET GESTION DES OPÉRATIONS SUR TITRES ET VALEURS MOBILIÈRES</u>
  CE net Comptes permet au Client, sur option, la passation d'opérations sur titres financiers sous réserve de la signature préalable d'une convention de compte d'instruments financiers.

- GAMME DE SERVICES TRESEO
  Sous réserve de disponibilité, cette gamme de services permet d'accéder au(x) service(s) TRESEO souscrit(s) par le Client pour visualiser l'ensemble des informations dédiées à ces offres, accéder aux reportings et aux documents produits.

2.3.2.2 - Opérations sur les comptes

- VIREMENTS
  Les Personnes habilitées pourront enregistrer des Comptes destinataires et créer des listes de destinataires selon leurs profils.

  Les Personnes habilitées pourront effectuer des virements unitaires de compte à compte ouverts dans les livres de la Banque au sein du périmètre des Comptes donneur d'ordre indiqué dans les Conditions Particulières, effectuer des virements SEPA, de manière unitaire ou multiple, également appelés virements groupés ou virements sur liste (sous réserve de disponibilité), des virements internationaux et des virements de trésorerie vers des Comptes destinataires préalablement enregistrés dans le Référentiel de l'abonnement. Dès la validation du ou des virements, via une authentification forte, les ordres sont enregistrés. Les ordres de virements à exécution immédiate sont irrévocables dès leur réception par la Banque.

  Le Client a la possibilité de révoquer un ordre de virement permanent ou à exécution différée dans les conditions indiquées dans la partie relative aux « Services de paiement » de sa convention de compte courant.

  Les ordres de paiement et les opérations qui en découlent sont soumis aux conditions de traitement habituelles en vigueur dans la Banque, à la date de l'opération et objet de la convention de compte courant régularisée par acte séparé par le Client, sauf conditions spécifiques prévues dans les conditions particulières de la convention de compte courant, et/ou dans les Conditions Particulières du Contrat.

  Le Client peut suivre les opérations transmises dans le suivi des ordres.

  Le montant maximum de virement accepté par la Banque est indiqué au Client par le Service ou, le cas échéant, aux Conditions Particulières ou encore dans tout autre document destiné au Client. Ces montants limites peuvent aussi être fournis par la Banque, à la demande du Client.

  Pour garantir le bon déroulement de ses virements, il est recommandé au Client de contrôler ses bénéficiaires existants ou lors de l'ajout d'un bénéficiaire sur sa liste, en s'assurant que les noms des bénéficiaires correspondent exactement aux noms enregistrés sur leurs comptes bancaires :
  - Le nom et le prénom lorsque le bénéficiaire est une personne physique ;
  - La raison sociale ou le nom commercial lorsque le bénéficiaire est une personne morale (entreprises, associations, ...).

  Ces informations sont disponibles sur le Relevé d'identité bancaire (RIB) du bénéficiaire. Il convient de ne pas utiliser des abréviations ou des surnoms. Toute différence, même minime, ou toute autre information que le prénom et le nom ou la raison sociale ou le nom commercial, pourrait entraîner une non-concordance dans le cadre du service de vérification du bénéficiaire décrit ci-après.

  La mise à jour de la liste des bénéficiaires relève de la propre initiative du Client. La Banque ne contactera jamais le Client (par téléphone ou par un autre moyen) pour lui proposer de l'accompagner dans cette démarche.

  Spécificités applicables aux virements multiples (sous réserve de disponibilité) : Le virement multiple correspondant à un ensemble de virements SEPA saisis de manière groupée dans l'Espace de banque à distance du Client et pouvant porter sur un ou plusieurs bénéficiaires. Les virements composant un virement multiple font l'objet d'une validation unique par authentification forte. Cette validation vaut consentement du Client à l'exécution de l'ensemble des ordres de paiement composant le virement multiple. Avant validation, un récapitulatif des virements saisis est présenté au Client, incluant notamment le nombre d'opérations, les bénéficiaires concernés, les montants de chaque virement ainsi que le montant total. Le Client peut, selon les fonctionnalités disponibles, choisir les modalités de comptabilisation des virements : une comptabilisation globale correspondant à un débit unique du montant total des virements, ou une comptabilisation détaillée correspondant à un débit distinct pour chacun des virements composant l'opération et pouvant donner lieu à des dates d'exécution différentes pour chacun des virements.

  Le Client est informé que la validation d'un virement multiple entraine l'exécution simultanée de plusieurs opérations de paiement et qu'il supporte les conséquences des erreurs affectant un ou plusieurs ordres saisis dans ce cadre.

  Vérification du bénéficiaire - Virements SEPA classiques et instantanés (service permettant de renforcer la sécurité des virements et de réduire les risques d'erreurs et de fraudes)

  - Principes généraux
  Conformément au Règlement (UE) 2024/886 du 13 mars 2024, la Banque, en tant que banque du payeur, procède à la vérification du bénéficiaire auquel le Client a l'intention d'envoyer un virement SEPA classique ou instantané. Ce service vérifie la concordance entre l'IBAN du compte du bénéficiaire et le nom de ce dernier. Etant précisé que le nom du bénéficiaire

correspond au nom et prénom, dans le cas d'une personne physique, au nom commercial ou à la dénomination sociale ou à un autre élément de données accepté par la Banque, dans le cas d'une personne morale.

Cette vérification est réalisée dès que le Client a complété les informations relatives au bénéficiaire, dans l'ordre de virement, et avant qu'il autorise le virement dans son Espace de banque à distance, accessible via le site internet ou l'Application mobile de la Banque.

Pour les virements différés et permanents, la vérification est effectuée lors de la constitution de l'ordre de virement par le Client et non à chaque échéance du virement.

Aucune vérification n'est effectuée lorsque le Client ajoute le compte d'un bénéficiaire dans sa liste de bénéficiaires de virements.

Ce service est fourni au Client à titre gratuit.

- Résultats de la vérification

A la demande de la Banque, cette vérification est effectuée par le prestataire de services de paiement du bénéficiaire qui transmet sa réponse à la Banque.

En cas de concordance, le parcours de virement se poursuit.

Dans les autres cas, le résultat de la vérification des bénéficiaires est mis à disposition du Client par la Banque, avant la validation de l'ordre saisi. Ce résultat n'est valable qu'au moment de la mise à disposition du rapport par la Banque au Client, et ne saurait en aucun cas prévaloir pour l'avenir.

En cas de concordance partielle et de non-concordance, la Banque informe le Client que l'autorisation du virement pourrait conduire à ce que les fonds soient virés sur le compte d'un autre bénéficiaire que celui auquel le Client souhaite transmettre les fonds.

- En cas de concordance partielle, la Banque communique au Client le nom du bénéficiaire associé à l'IBAN qu'il a fourni. Le Client a alors la possibilité :
  - Soit, de corriger le nom du bénéficiaire et d'autoriser le virement. Le nom du bénéficiaire est ainsi automatiquement modifié dans la liste de bénéficiaires de virements du Client.
  - Soit d'autoriser le virement sans modifier le nom du bénéficiaire.
  - Soit d'annuler le virement.

- En cas de non-concordance, le Client en est immédiatement informé. La Banque ne lui donne aucune information sur le bénéficiaire. Le Client a alors la possibilité :
  - Soit, d'annuler le virement et s'il le souhaite de modifier le nom du bénéficiaire dans sa liste de bénéficiaires de virements, et de réémettre un nouveau virement qui sera soumis à une nouvelle vérification du bénéficiaire.
  - Soit, d'autoriser le virement sans corriger le nom du bénéficiaire dans sa liste de bénéficiaires.

Le Client est également informé lorsque la banque du bénéficiaire ne permet pas de vérifier le nom du bénéficiaire associé à l'IBAN. Le Client pourra alors annuler le virement ou l'autoriser.

Si, malgré les alertes, le Client autorise le virement, la Banque l'informe :
- Que le virement est considéré comme exécuté au profit du bon bénéficiaire ;
- Qu'elle ne peut pas être tenue responsable de l'exécution de ce virement au profit d'un mauvais bénéficiaire ;
- Qu'il n'a pas droit au remboursement de ce virement pour opération mal exécutée.

De même, la Banque n'est pas responsable de l'exécution d'un virement SEPA en faveur d'un mauvais bénéficiaire, sur la base d'un IBAN inexact communiqué par le Client, pour autant que la Banque ait satisfait à ses obligations au titre du service de vérification du bénéficiaire.

En cas de non-respect par la Banque ou un prestataire de services d'initiation de paiement de ses obligations en matière de vérification du bénéficiaire, entraînant une opération de paiement mal exécutée, la Banque restitue sans tarder au Client le montant du virement SEPA et, le cas échéant, rétablit le compte dans la situation qui aurait prévalu si l'opération n'avait pas eu lieu.

Si le compte du bénéficiaire est clôturé, le Client en est également informé et le virement ne peut pas être exécuté.

- Description du service lorsque la Banque agit en tant que banque du bénéficiaire

A la demande de la banque du payeur, la Banque est tenue de vérifier la concordance entre l'IBAN du compte et le nom du bénéficiaire, fournis par le payeur. La Banque informe la banque du payeur du résultat de cette vérification. En cas de concordance partielle, la Banque a l'obligation réglementaire de communiquer à la banque du payeur le nom du Client bénéficiaire du virement.

- PAIEMENT D'EFFETS DE COMMERCE
  CE net Comptes permet au Client d'être informé de la présentation des lettres de change et des billets à ordre à honorer et, le cas échéant, de gérer ces derniers. L'ensemble de ces fonctionnalités sont réalisées conformément aux dispositions prévues dans la convention de compte courant qu'il a signée.

- CONSULTATION DES ENCOURS DAILLY
  CE net permet au Client, la consultation détaillée des encours de créances Dailly (par Avance ou en Garantie), sur les comptes cédants compris dans le périmètre de son abonnement. La faculté de consultation de la part du Client ne présume pas de l'octroi d'une ligne de cession de créances professionnelles (DAILLY).

- CESSION DÉMATÉRIALISSÉE DE CRÉANCES PROFESSIONNELLES
  Sous réserve que le Client dispose d'une ligne de cession de créances professionnelles octroyée par la Banque, CE net permet au Client et aux Utilisateurs de céder des créances dématérialisées (par Avance ou en Garantie), sur les comptes cédants compris dans le périmètre de son abonnement, en permettant notamment le dépôt et la signature de ses bordereaux de cession dématérialisés (Service e-Dailly).

- PARAFEUR
  Il s'agit d'un espace dédié à la validation unitaire ou groupée (au moyen d'une Authentification forte) des ordres de paiement saisis ou transmis. La validation peut également être différée.

  Sous réserve de disponibilité du service, tous les ordres saisis en ligne ou transmis par fichiers sont agrégés dans cette rubrique. Les Utilisateurs pourront confirmer des ordres unitairement ou en masse, seuls ou en groupe, relancer des valideurs, visualiser l'état du traitement des ordres par la Banque directement à partir de l'historique d'ordres.

2.3.2.3 - Opérations de financement

CE Net Compte permet la consultation des contrats de crédits court, moyen, long terme ainsi que des engagements par signature. Outre la consultation des crédits octroyés au Client, les personnes dûment habilitées à représenter le Client pourront signer électroniquement une opération en lien avec ses crédits.

2.3.2.4 - Contrat d'assurance

Le Client peut visualiser les références des contrats d'assurance souscrits auprès de la Banque.

2.3.2.5 - Moyens de paiement

- PILOTAGE DE LA CARTE A USAGE PROFESSIONNEL ET CONSULTATION DES OPÉRATIONS
  CE Net Comptes permet à un porteur de carte à usage professionnel, Utilisateur de CE net, de pouvoir effectuer le pilotage de la carte Business dans les conditions précisées au contrat porteur carte à usage professionnel signé avec la Banque.

  Sous réserve de disponibilité, un Administrateur pourra également augmenter temporairement le plafond de la carte d'un des porteurs sous réserve que la carte soit incluse dans le périmètre de l'abonnement.

  L'utilisation de ces fonctionnalités par la Personne habilitée s'effectue sous sa responsabilité. Elle pourra nécessiter une Authentification forte par Sécur'Pass que la Personne habilitée doit avoir préalablement activé dans l'Application mobile.

  Uniquement depuis l'Application mobile, dans la rubrique lui permettant de gérer sa carte, la Personne habilitée titulaire d'une carte à usage professionnel peut également enrôler sa carte dans la solution de paiement mobile Apple Pay ou Google Pay sur le même smartphone où il a téléchargé cette Application mobile. Lors de cet enrôlement, il devra s'authentifier par Sécur'Pass.

  A partir de cette même rubrique et uniquement depuis l'Application mobile, le Client, par l'intermédiaire de l'Administrateur sous réserve que ce dernier y soit dûment habilité, peut souscrire au service e-Cartes le cas échéant pour une ou chacune de ses cartes à usage professionnel ou pour une carte dont une Personne habilitée est titulaire. Une fois souscrit, ce service permet à la Personne habilitée titulaire de la carte de créer une ou plusieurs e-Cartes, depuis l'Application mobile, afin de payer des achats sur internet, sans communiquer les données de sa carte physique.

  Sous réserve d'éligibilité du Client et de disponibilité de cette fonctionnalité, l'Administrateur, sous réserve que ce dernier y soit dûment habilité, peut demander la souscription d'une carte à usage professionnel pour lui-même ou un autre collaborateur du Client selon un parcours dédié, depuis CE net, rubriques Pilotage de la carte ou Souscrire, avec ensuite signature électronique à distance des conditions particulières du contrat porteur carte professionnelle par le porteur de la carte à usage professionnel.

- OPPOSITION SUR CHÉQUIERS ET CARTES BANCAIRES
  CE net Comptes permet au Client d'obtenir les informations utiles aux modalités d'opposition pour les chèques et cartes bancaires.
  Le cas échéant, toute opposition devra être complétée, dans les quarante-huit (48) heures, des documents sollicités à adresser à la Banque.

- COMMANDE DE CHÉQUIER
  CE net Comptes permet au Client, à condition d'y avoir été habilité et d'être équipé d'un moyen d'Authentification forte (cf. article 5), de commander en ligne des chéquiers, si celui-ci n'a pas opté pour le renouvellement automatique.

- COMMANDE DE BORDEREAUX DE REMISE DE CHÈQUES
  CE net Comptes permet au Client, à condition d'y avoir été habilité, de commander en ligne des bordereaux de remise de chèques qui seront livrés à l'adresse précisée lors de la souscription du service auprès de la Banque.

2.3.2.6 - Autres services

- DIGITAL SHARE
  Le service d'échange de document permet aux Personnes habilitées de visualiser les demandes de documents de la Banque et suivre leur état d'avancement, et de déposer des documents à destination de la Banque sous format électronique *(notamment pdf, jpeg, ...)*.

  La Banque notifie l'Utilisateur Principal et l'Administrateur par message électronique lors de la création d'une demande de document, d'une relance ou lors du rejet d'un document déposé. La Banque est avertie dès qu'un document est déposé par l'Utilisateur Principal ou un Administrateur.

- MESSAGERIE SÉCURISÉE INTERNET OU MSI (CONDITIONS GÉNÉRALES D'UTILISATION)

  - **Description du service**
    Dans le cadre de l'abonnement à CE net souscrit par le Client, chaque Utilisateur a accès à une messagerie électronique dédiée dans l'environnement sécurisé de CE net, dénommée la « Messagerie Sécurisée Internet » (ci-après « MSI »). Le Client et les Utilisateurs sont informés que le premier accès à la MSI vaut acceptation des présentes Conditions Générales d'Utilisation dont ils doivent prendre connaissance au préalable. Les messages sont consultables par les Utilisateurs pendant un délai de 90 (quatre-vingt dix) jours à compter de leur réception.

  - **Accès à la Messagerie Sécurisée Internet**
    La MSI est exclusivement accessible aux Utilisateurs de CE net. Toute utilisation du Service sera réputée avoir été effectuée par un Utilisateur. Le Client est informé qu'en résiliant son abonnement à CE net, il met fin à l'accès à la Messagerie Sécurisée Internet de tous les Utilisateurs. Dans ce cas, le Client et les Utilisateurs perdent définitivement l'accès aux messages conservés jusqu'alors dans leur MSI. Il appartient au Client d'alerter en temps utile l'ensemble des Utilisateurs des conséquences de la résiliation de l'abonnement CE net sur leur MSI.

    La suppression d'un Utilisateur de l'abonnement CE net du Client entraine immédiatement la fermeture et la suppression de la MSI de cet Utilisateur. Il appartient au Client de prendre préalablement ses dispositions.

  - **Fonctionnalités du service**

    - Interlocuteurs des Utilisateurs :
      La MSI permet à l'Utilisateur d'adresser, ou de recevoir, des messages électroniques en direction, ou en provenance, d'une ou plusieurs personnes du réseau des Caisses d'Epargne dont la liste est définie par la Banque.

    - Notification d'un nouveau message dans la Messagerie Sécurisée Internet :
      Sous réserve de la disponibilité de ce service dans la Banque et de la déclaration préalable d'une adresse électronique personnelle valide à usage professionnel, l'Utilisateur peut recevoir une notification électronique des nouveaux messages parvenus dans sa MSI. La Banque n'est pas responsable de la saisie erronée des données personnelles de l'Utilisateur, du filtrage anti-spam abusif du transport des données, de la qualité et de la disponibilité des réseaux de télécommunication, ni des interruptions pour les interventions de maintenance, par suite de cas fortuits ou de force majeure et, en particulier, celles qui se produisent à la suite d'un mauvais fonctionnement du matériel de l'Utilisateur ou du réseau de télécommunications.
      La Banque dégage sa responsabilité des difficultés associées au contrat passé entre le Client et son fournisseur d'accès.
      La MSI est un vecteur de communication des notifications que le Client recevra pour l'informer de la mise à disposition des relevés/documents électroniques dans son espace CE net.

    - Suppression des messages :
      L'Utilisateur a la possibilité de supprimer de la MSI des messages électroniques émis ou reçus par lui. Dans ce cas, aucune restauration de ces messages ainsi supprimés ne sera possible ultérieurement. Par ailleurs, les messages électroniques transmis et reçus resteront disponibles pendant 90 (quatre-vingt-dix) jours, au-delà de ce délai, ils sont purgés.

    - Limite à la capacité de stockage :
      La MSI attribuée à l'Utilisateur est limitée dans sa capacité de stockage en raison des contraintes techniques et/ou de sécurité retenues par la Banque, susceptibles d'évoluer dans le temps. L'espace de messagerie effectivement utilisé est visible dans la Messagerie sécurisée de l'Utilisateur. En cas de dépassement de cette capacité de stockage, la Banque pourra

être amenée à supprimer les messages diffusés en automatique, à caractère commercial ou bien relatifs à la gestion des comptes de l'Utilisateur.

- **Contenu des messages**

  - Règles d'utilisation de la MSI :
    La MSI est exclusivement un service de dialogue entre l'Utilisateur et des interlocuteurs de la Banque. L'Utilisateur s'engage à n'utiliser la MSI que dans le cadre strictement limité à la relation bancaire définie par le Service CE net. Aussi, l'Utilisateur s'interdit de transmettre tout message, pièce jointe ou autre document qui n'aurait aucun lien direct, voire indirect avec l'objet de CE net. La MSI n'est pas destinée à la prise en compte des demandes relatives aux opérations bancaires, aux opérations sur instruments financiers et à l'inscription de comptes destinataires de virements. L'Utilisateur est tenu soit d'effectuer ses opérations conformément aux dispositions de CE net, soit de transmettre ses demandes à la Banque qui gère les comptes du Client. L'Utilisateur devra faire un usage raisonnable du service, notamment quant au contenu, à la fréquence des messages envoyés ou à la taille ou au format des pièces jointes, toute autre utilisation pouvant notamment être à l'origine d'une saturation de l'infrastructure informatique de nature à mettre en péril la qualité et la continuité du service. En cas d'utilisation déraisonnable, la Banque se réserve le droit de mettre en demeure le Client, par tous moyens, de cesser une telle utilisation. A défaut de changement de sa part, la Banque se réserve le droit de résilier le Service, sans que le Client puisse prétendre à une quelconque indemnité, en raison notamment de la perte des messages contenus dans la MSI ainsi supprimée.

  - Traitement d'une demande formulée dans un message :
    En l'absence de réponse de l'interlocuteur dans un délai raisonnable, l'Utilisateur est invité à contacter la Banque par tout autre moyen. La prise en compte des demandes de mise à jour des données et des informations personnelles de l'Utilisateur pourra être conditionnée par la Banque à la présentation par le Client des pièces justificatives correspondantes.

- **Sécurité**
  L'Utilisateur est tenu de vérifier la qualité des documents électroniques joints à ses messages, en veillant notamment à ce qu'ils ne comportent pas de virus ou autres logiciels malveillants. La Banque se réserve le droit de supprimer les documents électroniques attachés aux messages échangés qui menaceraient directement ou indirectement l'intégrité de son système d'information. La Banque met en œuvre ses meilleurs efforts afin d'assurer la non-dangerosité des messages envoyés à l'Utilisateur via la MSI ; mais elle ne peut, compte tenu des aléas techniques, le garantir complètement. Il appartient, en conséquence, au Client et à l'Utilisateur de mettre en œuvre les mesures adéquates afin de préserver l'intégrité du poste informatique de l'Utilisateur. En tout état de cause, la Banque ne saurait être tenue responsable en cas de dommages causés au poste informatique de l'Utilisateur.

- **Archivage des messages par l'Abonné**
  La Banque rappelle au Client ainsi qu'aux Utilisateurs qu'il leur appartient de mettre en œuvre régulièrement les procédures de sauvegarde (copies d'écrans, copie du texte dans un document électronique, export dans un fichier au format PDF, etc.) adéquates afin d'archiver sur le système informatique du Client tous les documents ou messages stockés dans leur MSI, notamment afin de tenir compte de la possibilité pour la Banque de fermer, et de supprimer le cas échéant, l'accès au Service ou encore de supprimer des messages en cas d'atteinte à la capacité de stockage de ladite Messagerie. La Banque ne saurait être tenue pour responsable en cas de perte par le Client des documents et messages susmentionnés qui n'auraient pas été correctement sauvegardés.

- <u>ACCÈS FACILITÉ À CERTAINS SERVICES</u>
  CE net Comptes permet aux Utilisateurs ou le cas échéant au représentant légal seul, l'accès sans nouvelle Identification/Authentification à certains services proposés par la Banque (PulCEo Connect ...) et/ou d'autres entités du Groupe BPCE à condition pour le Client d'y avoir souscrit et d'y être habilité.

  Le Client reconnait que toute opération réalisée sur l'un de ces services et consécutive à ce dispositif d'accès lui sera opposable et l'engagera à l'égard des entités proposant ces services. Cette opération sera soumise aux conditions générales d'utilisation de ces espaces.

2.3.3 - Services optionnels disponibles dans CE net Comptes

- <u>SUIVI DES OPÉRATIONS SWIFT GPI</u>
  Le service SWIFT - GPI permet au Client, sous réserves de souscription et d'habilitations, de consulter l'état d'avancement de certaines de ses opérations internationales.

- <u>SERVICE DIGITAL BOX</u>
  Le service « Digital Box » permet au Client et aux Personnes habilitées de télécharger et consulter sous forme électronique via l'abonnement CE net les relevés de compte et tous les documents dématérialisés disponibles. L'activation et la résiliation de ce service sont effectuées par le Client auprès de la Banque.

- SERVICE DE GESTION DE FACTURES

- **Description du service Gestion de factures**

Pour accéder au service de Gestion de factures, sous réserve de disponibilité de ce service, le Client doit être équipé du Service CE net Comptes ou CE net Remises et d'un compte courant professionnel.

Le Client peut souscrire le service de Gestion de factures via son Espace de banque à distance, le cas échéant, avec l'aide de son conseiller.

Seul l'Utilisateur principal peut souscrire et résilier le service de Gestion de factures, ainsi que, le cas échéant, modifier le niveau de services avec la tarification associée, sous réserve d'être habilité à ces fins par le Client et à engager le Client. Seules les Personnes habilitées peuvent utiliser le service de Gestion de factures, dans le périmètre et les limites qui leur ont été attribués dans le cadre du Service, mais aussi dans le cadre du service de Gestion de factures.

Dans le cadre de la mise en œuvre de la réforme sur la facturation électronique, le Client peut, via le service de Gestion de factures, choisir IPT Technologie, en tant que plateforme agréée par la Direction Générale des Finances Publiques. A cette fin, le Client doit sélectionner la rubrique dédiée dans le service et signer un mandat désignant IPT Technologie comme plateforme agréée. Le Client entre ainsi en relation contractuelle directe avec IPT Technologie.

Les services fournis par IPT Technologie en sa qualité de plateforme agréée, disponibles via le service de Gestion de factures, sont les suivants, conformément à la réforme sur la facturation électronique :
- réception et transmission de factures électroniques entre entreprises établies en France et assujetties à la TVA française et transmission des données liées à ces factures à l'administration fiscale,
- mise au bon format normalisé des factures électroniques à transmettre ;
- production et transmission à l'administration fiscale des e-reportings exigés par la réforme portant sur :
  - les données des transactions (ou e-reporting de transaction) concernant les opérations de ventes et/ou de prestations de service avec des personnes non assujetties par exemple des particuliers, ou des transactions avec des opérateurs établis à l'étranger ;
  - les données de paiement ou données d'encaissement (ou e-reporting de paiement) concernant les opérations dont la TVA est exigible à l'encaissement.

Le Client est informé que la résiliation ou l'expiration du service de Gestion de factures entraîne automatiquement la résiliation des services fournis par IPT Technologie en qualité de plateforme agréée.

Si le Client choisit IPT Technologie comme plateforme agréée, les principales fonctionnalités disponibles dans le service de Gestion de factures sont les suivantes (selon le niveau de service qu'il choisit, le Client peut ne pas disposer de certaines fonctionnalités) :
- Création de devis et édition de factures pour ses propres clients, avec possibilité d'y insérer un lien de paiement afin d'être réglé par virement : Le Client peut créer des devis, éditer des factures avec ou sans lien de paiement et bénéficier de services connexes, tels que le suivi des paiements en temps réel et les relances automatiques des impayés. A ce titre, le Client, mandant, confie à la Banque, mandataire, dans le respect des règles économiques et fiscales applicables, l'établissement et l'émission de ses factures. A cet égard, le Client donne expressément mandat à la Banque d'établir en son nom et pour son compte des factures originales afférentes à tout type de prestations de services ou d'achat et ce conformément à la réglementation fiscale et économique en vigueur, et en particulier les dispositions des articles 289, I-2 et 242nonies, I (Annexe 2) du Code général des impôts. Il incombe au Client d'indiquer à la Banque son assujettissement ou non à la TVA et toutes les informations nécessaires à l'établissement de ses factures. Le Client reste responsable de ces informations. Lesdites factures seront à la disposition du Client dans le service de Gestion de factures.
  Pour les factures électroniques relevant de la réforme sur la facturation électronique, le service de Gestion de factures permet au Client de transmettre la facture à son client via la plateforme agréée IPT Technologie. Pour les autres factures, le service de Gestion de factures permet au Client de les transmettre directement à ses clients par courrier électronique.
- Import et collecte automatisée des factures fournisseurs et paiement : La Banque procède à la collecte automatique des factures fournisseurs du Client ne relevant pas de la réforme sur la facturation électronique, à partir (i) de l'adresse de courrier électronique du Client et/ou (ii) de son espace client sur les sites fournisseurs. Pour les factures électroniques relevant de la réforme sur la facturation électronique, le Client les reçoit dans le service de Gestion de factures, via la plateforme agréée IPT Technologie. Pour l'ensemble des factures, la Banque procède à l'extraction des informations clés qui y figurent. Le Client a la possibilité de payer ses factures via le service de Gestion de factures.
- Le stockage : La Banque propose des espaces de stockage permettant au Client de stocker tout type de document.
- Le rapprochement bancaire assisté et la synchronisation des comptes bancaires externes (voir ci-dessous) : le Client peut comparer les factures avec les transactions bancaires effectuées depuis le(s) compte(s) courant(s) professionnel(s) détenus auprès de la Banque, mais aussi auprès d'autres banques, sous réserve d'avoir inclus ces autres comptes dans le périmètre de la synchronisation.
- Gestion des notes de frais : la Banque met à la disposition du Client et de ses collaborateurs une application mobile dédiée aux notes de frais permettant de les scanner et de les ajouter dans le service, à télécharger sur les appareils compatibles depuis les espaces de téléchargement d'applications (Google Play, Apple Store, etc…). La Banque procède ensuite à l'extraction et à la saisie automatique des informations relatives aux montants et aux dates desdites notes de frais.

- Suivi du prévisionnel de trésorerie : selon le niveau de service choisi, le Client peut suivre l'évolution de sa trésorerie, ses budgets et objectifs
- Gestion et export des documents et écritures vers les logiciels comptables et possibilité d'accès externalisé à l'espace gestion de factures pour le comptable du Client : le Client peut inviter son comptable externe à accéder au service de Gestion de factures en renseignant les coordonnées et l'adresse électronique de ce dernier. Cette invitation est entièrement sous la responsabilité du Client qui peut à tout moment révoquer l'accès accordé. Le comptable dispose d'un accès limité via une interface dédiée, lui permettant d'effectuer des actions spécifiques liées à la préparation de la comptabilité, comme par exemple consulter les opérations/justificatifs comptables et bancaires et les télécharger si besoin. Le comptable ne peut pas créer ou ajouter d'autres accès au sein du service de Gestion de factures, ni accéder à d'autres fonctionnalités de l'Espace de banque à distance du Client. Il n'a pas non plus la possibilité de procéder à des paiements ou à des encaissements, ni d'effectuer d'autres opérations qui pourraient engager l'entreprise.
- « Paiement des factures fournisseurs », « Encaissement via lien de paiement inséré dans les factures clients » et « Synchronisation des comptes bancaires externes », disponibles dans le service de Gestion de factures, s'appuient sur :
  - les services d'information sur les comptes, également appelés agrégation de comptes (intitulés « Synchronisation des comptes bancaires » dans le service de Gestion de factures) et d'initiation de paiement fournis par Perspecteev (Bridge) ;
  - le service d'information sur les comptes fournis par Powens.

  Afin d'accéder à ces services, le Client sera redirigé par un lien URL vers le site internet de ces prestataires et entrera en relation contractuelle directe avec celui-ci conformément à leur conditions générales et politique de confidentialité rendues accessibles et qui devront être acceptées préalablement à l'utilisation de ces services. Les services sont fournis de manière indépendante par chaque prestataire. Le Client est informé que la résiliation ou l'expiration du service de Gestion de factures entraîne automatiquement la résiliation des services fournis par ces prestataires.

Le service ne peut être rendu que pour : des documents digitalisés selon un format approprié ; des données rédigées dans l'alphabet latin et/ou contenant une numérotation décimale ; des données issues de documents envoyés ou reçus à partir des formats de fichiers suivants : .jpg, .jpeg, .png, .tiff, .tif, .gif, .pdf, .txt, .docx, .pptx, .xlsx, .doc, .xls et Factur-X pour les factures électroniques reçues et transmises via la plateforme agréée IPT Technologie. La Banque ne peut pas garantir l'extraction exacte des données et informations issues de documents envoyés ou reçus sous d'autres systèmes et/ou formats que ceux évoqués ci-dessus.

Si le Client ne choisit pas IPT Technologie comme plateforme agréée, le Client ne pourra pas bénéficier des fonctionnalités suivantes, via le service de Gestion de factures, pour les factures électroniques relevant de la réforme sur la facturation électronique :
- les éditer et les transférer à ses clients éligibles à cette réforme ;
- les recevoir de ses fournisseurs éligibles à cette réforme ;
- transférer les données de ces factures à l'administration fiscale.

De même, il n'y aura pas transmission électronique à l'administration fiscale des e-reportings de transaction et de paiement précités.

- **Exclusions de responsabilités**

Les exclusions de responsabilité qui suivent sont sans préjudice des autres stipulations en vertu du Contrat.

Le Client reconnait et accepte que la Banque n'est pas responsable des services fournis par des prestataires tiers d'information sur les comptes, également appelés agrégation de comptes (intitulés « Synchronisation des comptes bancaires » dans le service de Gestion de factures) et d'initiation de paiement. En particulier, la Banque ne saurait être responsable des dysfonctionnements de ces services, de la sécurité de ces services, et/ou encore de la fréquence de la mise à jour par les prestataires tiers des informations restituées dans le service de Gestion de factures de l'Espace de banque à distance du Client.

Le Client reconnait et accepte que la Banque n'agit, dans le cadre de la fourniture de ces services, ni en qualité de conseiller, ni en qualité de comptable et que le service ne constitue pas des conseils financiers. Le Client est seul responsable du respect de ses obligations comptables et fiscales, en ce compris de ses obligations de conservation des données comptables et fiscales, et plus généralement des obligations imposées par la règlementation française et européenne.

Le Client reconnaît et accepte que la Banque n'est pas responsable des services fournis par IPT Technologie en sa qualité de plateforme agréée, dans le cadre du service de Gestion de factures. En particulier, la Banque ne saurait être responsable des dysfonctionnements et de la sécurité de ces services, et plus généralement du non-respect par IPT Technologie de son rôle et de ses obligations au titre de sa qualité de plateforme agréée, dans le cadre de la réforme sur la facturation électronique.

- **Souscription du service de Gestion de factures et modification du niveau de service**

Le Client souscrit le service en choisissant le niveau de service avec la tarification associée, adapté à ses besoins. Les cinq niveaux de service de Gestion de factures sont mentionnés dans le parcours de souscription, via l'Espace de banque à distance du Client, ainsi que dans les Conditions tarifaires applicables au Client.

Le Client peut visualiser le niveau de service qu'il a choisi dans la rubrique « Offre détenue » et changer à tout moment de niveau de service en cliquant sur le bouton prévu à cet effet dans cette rubrique.

La souscription du service et la modification du niveau de service sont effectuées en ligne par le Client et prennent effet immédiatement. Le Client en reçoit la confirmation à l'écran ainsi que par email à l'adresse électronique communiquée par le client à la Banque.

La Banque se réserve la possibilité de refuser la souscription du service en cas de souscriptions ou de résiliations successives multiples.

- **Conditions tarifaires**
  Le service est souscrit sous forme d'abonnement mensuel dont le montant est fonction du niveau de service choisi. Le Client pourra accéder aux différentes fonctionnalités incluses dans le niveau de service choisi et dans les limites qu'il prévoit. En cas de dépassement de ces limites : nombre de factures et/ou du nombre d'utilisateurs pour les notes de frais et/ou nombre de banques inclus dans la synchronisation des comptes bancaires prévues dans le niveau de service souscrit, des frais supplémentaires seront facturés. Le Client peut suivre sa consommation directement depuis le service et a la faculté de changer de niveau de service à tout moment.

  La tarification du niveau de service et les frais additionnels en cas de dépassement des limites, sont définis aux Conditions tarifaires de la Banque applicables au Client, disponibles dans la brochure tarifaire accessible depuis le site internet de la Banque ou auprès de l'agence.

  L'abonnement sera facturé mensuellement, à terme échu, à la date anniversaire de la souscription du service. Les éventuels frais additionnels en cas de dépassement des limites seront facturés à terme échu le mois suivant.

- **Durée et résiliation du service de Gestion de factures**
  Le service est souscrit pour une durée indéterminée.

  Le Client peut mettre fin au service à tout moment et sans frais, en contactant l'assistance du service de Gestion de factures via son Espace de banque à distance pour formaliser sa demande de résiliation.

  La résiliation du service interviendra à la date anniversaire de la souscription du service.

  La Banque peut également résilier le service à tout moment. Le Client en sera informé par lettre recommandée avec avis de réception. Cette résiliation prendra effet un mois après l'envoi de cette information.

  Le Client est informé que la résiliation du Service de banque à distance ne permet plus d'accéder au service de Gestion de factures, et entraîne sa résiliation automatique, ainsi que la résiliation automatique des services fournis par IPT Technologie en qualité de plateforme agréée.

  Après la résiliation du service, il ne sera plus possible de l'utiliser, notamment aucun document ne pourra plus être numérisé ni téléchargé. Il appartient donc au Client de procéder à la sauvegarde des documents nécessaires avant la résiliation effective du service.

- GESTION MULTI-SOCIÉTÉS
  Sous réserve de disponibilité, la fonctionnalité gestion multi-sociétés permet au Client d'accéder via son Espace de banque à distance aux comptes d'une autre société appartenant au même groupe, qui le mandate en ce sens afin de consulter les comptes désignés de cette dernière et, le cas échéant selon le contenu du mandat, d'effectuer sur ceux-ci les opérations proposées dans le Contrat, dans les limites et selon les modalités qu'ils prévoient.

2.4 - CE net Remises

CE net Remises permet au Client d'effectuer, par l'intermédiaire des Personnes habilitées à utiliser le Service, les principales fonctionnalités décrites ci-après (la liste n'étant pas exhaustive). En souscrivant à l'offre CE net Remises, le Client a accès à l'ensemble des fonctionnalités présentes dans l'offre CE net Comptes.

2.4.1 - Gestion des accès aux Services CE net Remises (saisie, dépôt et relevés)

L'accès des Utilisateurs à CE net Remises est paramétré lors de la souscription dans les Conditions Particulières mais aussi via son espace personnel CE net à partir de l'onglet « Paramétrage », en cliquant sur « gestion des utilisateurs ».

2.4.2 - Déposer et récupérer des fichiers EDI au format CFONB ou variable XML

CE net Remises permet le dépôt de remises de fichiers d'ordres de paiement sur le serveur EDI de la Banque et la récupération de fichiers de données informatisées (relevés de comptes, relevés d'opérations, accusé réception de fichiers, ...) conformes aux standards retenus par le CFONB.

2.4.3 - Saisir et gérer des fichiers EDI en ligne et prestations connexes

CE net Remises permet la saisie, la gestion et le suivi en ligne de fichiers de données informatisées, ainsi qu'un ensemble de prestations connexes :

- l'enregistrement des comptes des destinataires d'opérations,
- la création de listes de destinataires,
- la saisie et le contrôle des remises d'ordres de paiement et leur transfert à la banque,
- l'enregistrement et la modification d'une remise sauvegardée,
- la reprise des effets enregistrés en portefeuille en LCR,
- l'enregistrement des LCR/BOR détenus avant leur transfert dans une remise d'escompte ou d'encaissement,
- la création de listes de mandats de prélèvements SEPA,
- la saisie et le contrôle des remises de prélèvements SEPA à partir de liste de mandats préalablement enregistrés (cf.2.2.4),
- le suivi et la signature des ordres : la visualisation du fichier émis, le contrôle de son état, sa confirmation et sa suppression,
- le Parafeur : la confirmation des ordres par Signature électronique (Cf. article 5),
- la personnalisation de la dénomination d'un compte émetteur et du rang de présentation pour la saisie d'opérations.

2.4.4 - Gérer des mandats et créer des remises de prélèvements SEPA

CE net Remises permet la gestion des mandats de prélèvements SEPA :

- création et modification des mandats par saisie du Client ou par import des données du Mandat,
- génération manuelle ou automatique de la Référence Unique de Mandat (RUM),
- gestion des amendements liés aux modifications des données du mandat,
- gestion des rejets,
- création de listes de mandats de prélèvements SEPA,
- Création de base de mandats, pouvant être partagée entre différents Utilisateurs d'un même abonnement CE Net et habilités à saisir des prélèvements SEPA,
- création des remises de prélèvements SEPA à partir des listes de mandats, regroupées par date d'échéance.

Le Client aura préalablement signé la Convention d'émission des prélèvements SEPA CORE ou SEPA B2B (inter-entreprises).

Les mandats saisis ou importés par le Client dans le cadre des fonctionnalités du Service ainsi que les prélèvements saisis sont sous la responsabilité exclusive du Client. Le Client reconnait que la Banque n'est tenue à cet égard à aucun contrôle ou vigilance particulière. A ce titre, la Banque ne peut être tenue responsable des conséquences financières qui résulteraient d'une mauvaise indication des montants et/ou des comptes de destinataires, des mandats des ordres ou de rejet lors de la présentation des prélèvements à la banque destinataire.

En tout état de cause, le Client fait son affaire des litiges l'opposant à ses débiteurs, la Banque étant dégagée de toute responsabilité à cet égard.

La Banque s'engage à mettre à disposition de ses Clients un service de Gestion de Mandats et de création des prélèvements SEPA conforme aux règles édictées par l'EPC (European Payments Council) et le CFONB.

Pour bénéficier du service de gestion de mandat SEPA, le Client signera les conditions particulières adaptées qui préciseront, notamment, les fonctionnalités choisies ainsi que la tarification applicable.

2.5 - CE net EDI

CE net EDI est une offre à la « carte » proposant au Client de disposer de tout ou partie des Services CE net Remises et de réaliser ses opérations via un protocole de communication bancaire EBICS, SWIFTNet FileAct ou Pe SIT hors SIT moyennant la signature préalable d'un contrat spécifique à ces derniers par acte séparé.

CE net EDI permet aussi au Client de bénéficier du Collège de signature pour les opérations via un protocole de communication bancaire, sur simple demande de sa part. Le service Collège de signature, est un service permettant à l'Abonné d'inclure au sein d'un Collège un ou plusieurs Utilisateurs, permettant ainsi de déterminer les modalités de signature par le jeu de la composition des Collèges et des droits en cosignature.

Pour chaque opération déterminée, un seul Utilisateur par Collège de signature peut signer. La cosignature nécessite la signature de deux Utilisateurs de Collèges différents. Chaque Collège bénéficie des droits de signature définis par le Client.

Les droits des Utilisateurs et du ou des Collèges de signature seront définis dans les Conditions Particulières pour chacun des Services autorisés dans le périmètre de l'abonnement du Client CE net.

Par ailleurs, des Conditions Particulières spécifiques peuvent exister dans le cadre de certaine typologie de clientèle ou de volume de comptes très important.

2.6 - CE net COPRO

Dans le but de faciliter les échanges de documents et l'instruction des dossiers de financement de prêts collectifs copropriété en toute sécurité et confidentialité, la Banque met en œuvre une plateforme d'instruction et transfert de documents « CE net COPRO ». Cette plateforme permet aux syndics de copropriété de monter les dossiers de demande de financement de travaux dans le périmètre de leur abonnement.

ARTICLE 3 - PERSONNES HABILITÉES À UTILISER LE SERVICE

L'ensemble des Personnes habilitées qui sont mandatées à l'effet d'administrer des droits et/ou à l'effet d'utiliser CE net sont désignées aux Conditions Particulières et, le cas échéant, aux annexes du Contrat. L'Utilisateur Principal et les Administrateurs équipés d'un moyen d'Authentification forte, peuvent administrer les droits des Utilisateurs désignés aux Conditions Particulières.

Il est précisé que ces autorisations valent délégation de pouvoirs spécifiquement applicables au Contrat quels que soient les pouvoirs communiqués par ailleurs à la Banque, cette dernière n'ayant pas d'autres contrôles à effectuer.

La liste des Personnes habilitées est accessible à l'Utilisateur Principal et aux Administrateurs, lors de l'utilisation de CE net.

L'ajout, la suppression et/ou le changement de profil d'une Personne habilitée peut faire l'objet de la signature d'un avenant aux Conditions Particulières.

Le Service ne pourra pas être opérationnel pour une personne qui n'a pas été désignée dans la liste.

En cas d'ajout d'une Personne habilitée, il sera alors délivré à cette dernière un numéro d'Utilisateur, un code confidentiel et un dispositif d'Authentification forte utilisables dans les conditions du Contrat.

Il appartient au Client et/ou à l'Utilisateur Principal et/ou à l'Administrateur d'informer la personne dont l'habilitation a été supprimée ou modifiée.

Les stipulations du présent article s'appliquent sous réserve des limitations propres à l'offre souscrite par le Client, notamment s'agissant du nombre et des catégories de Personnes habilitées autorisées.

3.1 - L'Utilisateur Principal

L'Utilisateur Principal, désigné aux Conditions Particulières du Contrat :

- A la possibilité (i) d'accéder à tous les Services proposés par la Banque dans le cadre de CE net Comptes et CE net Remises, et compris dans le périmètre de l'abonnement prévu aux Conditions Particulières du Contrat, (ii) d'ajouter de plein droit (sans habilitation nécessaire) un nouveau Compte destinataire. L'Utilisateur Principal a tous les droits sur la gestion du Référentiel et des listes de Comptes destinataires,
- Est limité le cas échéant par les plafonds standard de saisie de virements établis par la Banque (ces plafonds sont susceptibles d'évolution et peuvent être modifiés par la Banque à tout moment) ou par les plafonds personnalisés qui peuvent être prévus aux Conditions Particulières sous réserve d'acceptation de la Banque.

De plus, il ne lui est pas possible d'agir sur le périmètre de l'abonnement sauf s'il est le représentant légal du Client ou dûment mandaté à cet effet par le Client.

L'Utilisateur Principal bénéficie également de toutes les fonctions d'Administrateur.

3.2 - L'Administrateur

Le ou les Administrateurs, désigné(s) aux Conditions Particulières du Contrat, ont en charge, sous réserve de disponibilité, l'ajout de nouveaux Utilisateurs et/ou l'attribution des droits aux Utilisateurs sur leur espace personnel CE net dans la limite du périmètre de l'abonnement indiqué aux Conditions Particulières et dans les limites des fonctions accessibles en ligne.

L'Administrateur peut :

- Consulter en ligne l'ensemble des Personnes habilitées à utiliser le Service et désignées aux Conditions Particulières,
- Gérer en ligne (affectation/modification/suppression) les droits des Utilisateurs sur les comptes du périmètre de l'abonnement, sur les fonctionnalités et le cas échéant sur les plafonds d'opérations. Lorsque la gestion des droits s'effectuera en prenant attache auprès de la Banque, de nouvelles Conditions Particulières devront être signées et annexées au présent contrat.
- Créer des Utilisateurs (sous réserve de disponibilité). La création d'un Utilisateur nécessite, auparavant de fournir à la Banque l'ensemble des documents requis que celle-ci pourra demander et de convenir avec la Banque du moyen d'authentification fort pour ce nouvel Utilisateur. Cette création est réalisée au travers de l'espace personnel CE net de l'Administrateur.
- Réaffecter en ligne un nouveau code confidentiel à la suite d'un blocage du code d'un Utilisateur.

Un Administrateur peut par ailleurs être également désigné Utilisateur (profil Administrateur Utilisateur). L'Administrateur Utilisateur bénéficie des fonctions d'Administrateur (article 3.2) et d'Utilisateur (article 3.3) sans pouvoir auto-administrer ses droits.

Ses droits sont gérés en ligne via CE net (Menu gestion des habilitations) par l'Utilisateur Principal, ou un autre Administrateur, ou le cas échéant paramétrés par la Banque à la suite de la demande du Client, formalisée par un avenant au contrat.

3.3 - Les Utilisateurs

Les Utilisateurs, désignés aux Conditions Particulières du Contrat, ne peuvent agir que dans le périmètre qui leur a été dévolu et dans les limites des fonctions accessibles en ligne. Leurs droits sont gérés en ligne via CE net (Menu gestion des habilitations) par l'Utilisateur Principal, ou un Administrateur, ou le cas échéant paramétrés par la Banque à la suite de la demande du Client, formalisée par un avenant au contrat.

L'Administrateur ou l'Utilisateur Principal a la possibilité de demander à la Banque de bloquer temporairement un Utilisateur.

Le Client peut également désigner ses collaborateurs porteurs de carte bancaire à usage professionnel en qualité d'Utilisateurs de CE net afin que ces derniers puissent réaliser, via un dispositif d'Authentification forte, des opérations de paiement par carte bancaire sur internet. Dans ce cadre précis, le Client reconnait que ces Utilisateurs n'auront accès à aucun des Services proposés par CE net à l'exception du module changement de mot de passe, de la Messagerie Sécurisée Internet et du dispositif d'Authentification forte Sécur'Pass Pro.

Enfin, dès qu'il souscrit une carte bancaire à usage professionnel pour un de ses collaborateurs, le Client autorise la Banque à donner automatiquement un accès limité à son Espace de Banque à distance, au titulaire de cette carte dans le but uniquement de permettre à ce dernier de :

- payer sur internet avec sa carte grâce à la saisie d'un code à usage unique, ainsi que de son mot de passe de connexion à l'Espace de Banque à distance ;
- s'enrôler à Sécur'Pass pour également payer sur internet avec sa carte et utiliser d'autres fonctionnalités et services liés à sa carte ;
- gérer sa carte et utiliser des services liés à sa carte depuis l'Espace de Banque à distance.

3.4 - Habilitation à la gestion du référentiel des Comptes destinataires

Il est possible aux Personnes habilitées équipées d'un moyen d'Authentification forte, de gérer le Référentiel des Comptes destinataires (ajout/modification/suppression).

Tous les Comptes destinataires vers lesquels des opérations peuvent être initiées sont enregistrés dans un Référentiel qui peut être consulté en ligne globalement ou partiellement par les personnes qui y sont autorisées. Ce Référentiel peut être composé, le cas échéant, de listes de comptes accessibles à condition d'y avoir été autorisé.

Le profil de chaque Utilisateur pour la gestion, l'utilisation et la consultation des Comptes destinataires est défini par l'Utilisateur Principal ou les Administrateurs dans le cadre de la gestion des habilitations. L'Utilisateur Principal bénéficie systématiquement du profil « Gestion du Référentiel et des listes ».

Trois profils de gestion et d'utilisation de ce Référentiel existent :

- Gestionnaire du Référentiel et des listes (Gestion du Référentiel) :
  - Utilisation et consultation de tous les Comptes destinataires du Référentiel,
  - Gestion du Référentiel et des listes de Comptes destinataires :
    - ajout/suppression de Comptes destinataires,
    - gestion des listes des Comptes destinataires et de leur attribution en consultation ou gestion des Utilisateurs, avec export possible du Référentiel (fichier au format csv).

- Utilisateur du Référentiel et des listes autorisées (Consultation du Référentiel) : Utilisation et consultation de tous les Comptes destinataires du Référentiel, avec en complément, accès aux listes sur lesquelles la personne a été autorisée par le gestionnaire du Référentiel et des listes.

- Utilisateur limité aux listes autorisées (Consultation des listes) : Utilisation et consultation uniquement des listes de Comptes destinataires sur lesquelles la personne a été autorisée par le gestionnaire du Référentiel et des listes.

Le Client garde la possibilité de demander par écrit à la Banque d'ajouter ou de supprimer des Comptes destinataires au périmètre de l'abonnement. Il devra fournir à la Banque, une demande d'enregistrement ou de mise à jour selon un formulaire mis à disposition par la Banque, reprenant notamment les coordonnées bancaires complètes des destinataires. Dans ce cas, la prestation pourra être soumise à tarification.

L'utilisation de profils de gestion permet d'assurer une sécurité concernant l'ajout/la modification/la consultation du Référentiel et/ou des listes. Il est ainsi possible d'habiliter des personnes uniquement à la fonction gestion du Référentiel des comptes destinataires afin d'assurer une sécurité lors de la saisie d'ordres.

Toutefois, il appartient au Client de s'assurer de l'authenticité des coordonnées bancaires qu'il reçoit avant toute intégration dans son Référentiel.

ARTICLE 4 - MOYENS MATÉRIELS ET TECHNIQUES D'ACCÈS À CE NET

4.1 - Principes

Le Client fait son affaire personnelle de l'acquisition ou de la location, de l'installation et de la connexion, de l'entretien et plus généralement de la garde de son matériel et de tous ses moyens techniques d'accès aux réseaux ou logiciels autres que ceux placés sous contrôle exclusif de la Banque ainsi que de leur protection au moyen d'un « Pare-feu » et / ou d'un antivirus à jour. Il en dispose sous son exclusive responsabilité. La Banque n'est pas responsable de l'évolution des logiciels, de leur mise à jour et du maintien des référencements.

Le Client doit assurer la sécurité et la confidentialité des données de son système d'information (comme par exemple, référentiel fournisseurs / référentiels Clients, etc..). Lors de toutes modifications de coordonnées bancaires de ses débiteurs, le Client s'assurera de l'exactitude de ces dernières.

Chacune des parties s'engage à communiquer à l'autre partie tout élément de nature à modifier les conditions de la réalisation de la prestation conformément aux dispositions stipulées dans les Conditions Particulières. Les parties réaliseront des tests préalables à la suite de ces modifications pour s'assurer de la continuité du Service.

4.2 - Logiciel de communication bancaire ou de paiement (EDI et API)

Le Service est accessible par un matériel compatible avec les normes télématiques (notamment, celles du centre serveur de la Banque) et Internet (ordinateur multimédia, téléphone compatible...), et leurs évolutions futures, relié au réseau de télécommunications.

Il appartient au Client de se procurer à ses frais et sous sa responsabilité les matériels et équipements appropriés (modem, cartes et logiciels de communication, logiciel d'agrégation et d'initiation de paiement...) ainsi que les moyens de communication (abonnements, accès à Internet...) nécessaires pour la transmission des ordres et la réception des relevés sur ses équipements.

Préalablement à tout échange de données informatisées et quel que soit le protocole utilisé, une phase d'initialisation est nécessaire pour assurer leur sécurité.

4.3 - Paramétrages et formats de fichier

Il appartient au Client de :

- se conformer aux paramétrages transmis par la Banque pour initier la communication bancaire,
- respecter les formats de fichiers selon la norme CFONB/NUG ou communiqués par la Banque, afin que leur syntaxe soit correcte. Ces formats, susceptibles d'évolutions à tout moment, sont disponibles auprès de votre Banque.

ARTICLE 5 - CONDITIONS D'ACCÈS ET DE SÉCURITÉ DE CE NET

La Banque met à disposition du Client des Instruments de paiement se caractérisant par des dispositifs comportant des Données de sécurité personnalisées et/ou un ensemble de procédures convenu et auxquels le Client a recours pour effectuer ses opérations notamment de paiement.

Chaque Utilisateur doit être équipé d'un dispositif d'Authentification forte requis par la Banque, pour l'accès au Service et son utilisation. Le Client est responsable de l'équipement en dispositif d'Authentification forte de chacun de ses Utilisateurs.

Les modalités d'accès, d'authentification et de gestion des habilitations prévues au présent article s'appliquent sous réserve des limitations propres à l'offre souscrite par le Client.

5.1 - Conditions d'accès et d'utilisation

Le Client / l'Utilisateur doit utiliser ses éléments d'identification et les dispositifs d'authentification mis en place par la Banque chaque fois qu'il en reçoit l'instruction, sous peine d'engager sa responsabilité.

La Banque pourra appliquer des exceptions, à l'application de l'Authentification forte, dans les conditions et selon les limitations prévues par le Règlement délégué UE 2018/389 du 27 novembre 2017, en particulier lors de l'accès à CE net et dans le cadre des virements permanents et des virements de compte à compte de l'Abonné.

Pour l'accès au Service, l'utilisation de ce dispositif d'Authentification forte, qui nécessite également la saisie d'un code spécifique, sera exigée par la Banque lors du premier accès et selon une périodicité déterminée par la Banque conformément à la réglementation applicable ou chaque fois que cela s'avère nécessaire pour raisons de sécurité.

5.1.1 - Accès par code confidentiel

A) PRINCIPE

Les Personnes habilitées accèdent au Service après s'être identifiées par la composition d'une triple clé formée du numéro d'Abonné (identifiant Client), d'un numéro d'Utilisateur et du code confidentiel.

Le numéro d'Abonné est attribué au Client et un numéro d'Utilisateur est fourni à chacune des Personnes habilitées désignée aux Conditions Particulières du Contrat par la Banque.

Pour permettre le premier accès au service, un code confidentiel provisoire est communiqué aux Personnes habilitées (soit par la Banque, soit par l'Utilisateur principal ou l'Administrateur dans le cas où les habilitations d'un Utilisateur sont gérées en ligne). Elles sont tenues de modifier ce code confidentiel provisoire par un code confidentiel qu'elles choisissent, lors de leur première connexion, selon la procédure indiquée par le Service. Ce mot de passe pourra être modifié, à tout moment, par la Personne habilitée à sa seule initiative et par la Banque pour des mesures de sécurité.

Après plusieurs tentatives infructueuses de composition du code confidentiel le dispositif d'accès au Service devient inopérant :

- lorsque le blocage concerne un Utilisateur, l'Utilisateur Principal et le ou les Administrateurs a (ont) alors la possibilité de procéder en ligne, à l'attribution d'un nouveau code confidentiel à l'Utilisateur. Une demande peut aussi être effectuée auprès de la Banque,
- lorsque le blocage concerne un Administrateur, l'Utilisateur Principal et ou les autres Administrateurs ont alors la possibilité de procéder en ligne, à l'attribution d'un nouveau code confidentiel. Une demande peut aussi être effectuée auprès de la Banque,
- lorsque le blocage concerne l'Utilisateur principal, il doit effectuer une demande de déblocage auprès de la Banque.

En cas d'oubli du code confidentiel, l'Utilisateur est invité à suivre le parcours « mot de passe oublié » accessible sur CE net.

B) CONFIDENTIALITÉ DES CODES

Le Client, l'Utilisateur Principal, le(s) Administrateur(s) dans le cadre des droits qu'ils gèrent, doivent informer les Personnes habilitées de leurs obligations de confidentialité découlant du Contrat notamment en leur communiquant les éléments ci-après.

Les Personnes habilitées prennent toute mesure raisonnable pour préserver la sécurité du numéro d'Abonné (identifiant Client), de leur numéro d'Utilisateur et de leur code confidentiel, ainsi que de tout élément d'authentification appartenant aux trois catégories ci-dessus. Les Personnes habilitées s'obligent à les tenir secrets et à ne les communiquer ou les remettre à quiconque, même à la Banque qui ne peut en avoir connaissance et ne les demandera jamais. Par ailleurs, les Personnes habilitées peuvent consulter la page « Sécurité » disponible sur le site Internet de la Banque.

Les Personnes habilitées doivent renouveler leur code confidentiel tous les 24 (vingt-quatre) mois. Il est conseillé de ne pas choisir un code confidentiel aisément décelable par un tiers (tel qu'une date de naissance par exemple).

Le numéro d'Utilisateur et le code confidentiel sont personnels aux Personnes habilitées. Elles en assument la garde, les risques, la conservation et la confidentialité, cela même à l'égard des salariés du Client ou des membres de leur famille. Ceci est une condition déterminante pour sécuriser les relations entre le Client et la Banque.

Toute personne qui en fera l'utilisation sera donc réputée autorisée par le Client et toutes les opérations seront réputées faites par lui. La Banque ne peut pas être tenue pour responsable en cas d'usage frauduleux ou abusif.

Il incombe au Client et aux Personnes habilitées de prendre les mesures nécessaires afin que la confidentialité de ces codes soit préservée et éviter ainsi toute fraude ou abus éventuel. Aussi, les Personnes habilitées doivent changer immédiatement leur code confidentiel, dès qu'elles ont connaissance de la perte, du vol, du détournement ou de l'utilisation frauduleuse de ce dernier, ou en cas de doute quant à la préservation de sa confidentialité, selon la procédure indiquée par le Service.

La Banque, l'Utilisateur Principal et les Administrateurs n'ont pas connaissance du code confidentiel que la ou les Personnes habilitées auront choisi. Néanmoins, l'Utilisateur Principal, et l'Administrateur, dans le cadre du périmètre d'habilitations qu'ils gèrent, peuvent, modifier le code confidentiel d'une personne habilitée, en cas de blocage ou du vol du code confidentiel de cette dernière en leur affectant un nouveau code confidentiel provisoire.

Cette obligation de confidentialité concerne également les codes à usage unique que l'Utilisateur serait amené à utiliser dans le cadre de la réalisation d'opérations nécessitant le recours à l'Authentification forte.

5.1.2 - Accès et validation par Authentification forte - Signature électronique des Opérations sensibles

Conformément à la réglementation en vigueur, la Banque met à la disposition du Client des moyens d'Authentification forte permettant d'accéder à CE net et d'y effectuer des Opérations sensibles avec un niveau de sécurité renforcée.

Le Client est dans l'obligation d'utiliser des moyens d'Authentification forts connus de la Banque et identifiés au Contrat, y compris aux fins d'utilisation de la Signature électronique pour ces opérations.

L'Authentification forte peut s'effectuer soit directement lors de la connexion au Service, puis lors de la validation des Opérations sensibles, soit uniquement lors de la validation des Opérations sensibles, si la connexion au Service a été réalisée par code confidentiel.

A) OPÉRATIONS SENSIBLES DE CE NET

Les Opérations sensibles de CE net sont les suivantes (sous réserve d'y être habilité) :

- ajout / suppression en ligne de nouveaux Comptes destinataires à la liste des Comptes destinataires déjà existants au Référentiel (gestion du Référentiel) ;
- gestion des habilitations en ligne par l'Utilisateur Principal ou par l'Administrateur ;
- commande en ligne des chéquiers (selon option des Caisses) ;
- validation d'un ordre de virement ;
- signature des remises d'ordres.

La liste des Opérations sensibles ci-dessus n'est pas exhaustive et est susceptible d'être complétée ou modifiée à tout moment par la Banque.

B) UTILISATION D'UN LECTEUR CAP

L'utilisation du service Sécurisation des Opérations en Ligne (SOL) par lecteur CAP pour s'authentifier et signer électroniquement une opération, le cas échéant, permet au Client de sécuriser les opérations effectuées en ligne.

La Banque préconise au Client de souscrire au service SOL par lecteur CAP par contrat séparé afin de sécuriser l'Authentification des Utilisateurs et les opérations effectuées en ligne notamment les Opérations sensibles indiquées ci-dessus. Les dispositions du contrat SOL par lecteur CAP viennent compléter celles du contrat CE net.

Les personnes amenées à utiliser SOL par Lecteur CAP doivent être habilitées par le Client à la fois dans le cadre de CE net et dans le cadre du contrat SOL.

C) UTILISATION D'UN CERTIFICAT ÉLECTRONIQUE

Les personnes autorisées par le Client peuvent s'authentifier et le cas échéant signer électroniquement dans le cadre du Service les opérations par l'usage d'un Certificat électronique dont elles ont fait l'acquisition par contrat séparé.

L'utilisation de ce Certificat nécessite l'installation du connecteur de sécurité TurboSign sur l'un des navigateurs internet compatibles : Firefox, Edge, Chrome.

L'Utilisateur du Certificat peut, avec ce Certificat et s'il y a été habilité dans le cadre du Service, réaliser des Opérations sensibles prévues par le Service CE net notamment celles mentionnées ci-dessus.

Une personne habilitée équipée d'un Certificat distribué par la Banque et enregistré dans les systèmes de cette dernière pourra l'utiliser dans le cadre des Services en ligne de CE net sans que le Client ait besoin d'en formaliser la demande auprès de la Banque.

Le Certificat électronique, s'il n'est pas souscrit auprès de la Banque, devra être au standard international en vigueur et faire partie de la liste des autorités de certification reconnues par la Banque et le cas échéant, être déclaré en annexe aux Conditions Particulières des présentes pour pouvoir être pris en compte par le Service (annexe « Déclaration de Certificat électronique »).

Le Client fait son affaire personnelle de la gestion (commande, renouvellement, révocation...) de son Certificat auprès de l'autorité de certification émettrice.

Le Client s'engage à informer, dans les meilleurs délais, par courrier recommandé AR, la Banque de tout changement de porteur du Certificat ou d'habilitation de ce dernier. Dans les 10 (dix) jours qui suivent la réception du courrier AR, une nouvelle déclaration de Certificat conforme sera signée entre les parties. Cette information s'applique également en cas de Certificats électroniques non nominatifs (tels que le Certificat 3Skey),

La Banque ne pourra être tenue responsable des conséquences liées à l'indisponibilité ou à la défaillance du Certificat électronique du Client.

La responsabilité de la Banque ne pourra en aucun cas être engagée en cas d'utilisation du Certificat par un porteur dont l'Identification ou l'habilitation ne lui a pas été communiquée dans les conditions susvisées.

Le Client s'engage à respecter les modalités d'utilisation d'un Certificat lors d'une Authentification forte ou de la Signature électronique, comme suit :

- Le Client ne doit introduire son Certificat sur son poste de travail qu'au moment où l'application d'Authentification ou de signature le demande et doit le retirer dès que l'Authentification ou la signature a été acceptée,
- En aucun cas, le Client ne doit laisser en permanence ou durant toute la durée de travail, le Certificat connecté à son poste de travail.

D) UTILISATION DE SOL SMS

L'utilisation du service SOL SMS pour s'authentifier, valider et/ou signer électroniquement une opération, le cas échéant, permet au Client de sécuriser les opérations effectuées en ligne.

Les Utilisateurs amenés à utiliser SOL SMS doivent être habilités par le Client dans le cadre de CE net.

La liste des fonctionnalités offertes par SOL SMS est susceptible d'évolution. Le Client et l'Utilisateur habilité en sont informés via la documentation s'y rapportant.

E) UTILISATION DE SECUR'PASS PRO

Le Client et chacune des Personnes habilitées peuvent, sous conditions, avoir accès depuis l'Application mobile, à Secur'Pass Pro, dispositif d'authentification forte permettant notamment sous réserve de leurs habilitations et dans la limite de celles-ci :

- d'accéder à CE Net et au(x) compte(s) courant(s) du Client en ligne,
- de sécuriser l'accès et l'utilisation de certains services,
- de valider certaines Opérations sensibles initiées depuis l'Espace de Banque à distance,
- de valider des opérations de paiement réalisées en ligne (virements) sur son Espace de Banque à distance et des opérations de paiement réalisées par carte bancaire sur internet (e-commerce),
- de s'authentifier lors de la souscription de produits et services commercialisés par la Banque par voie dématérialisée en ayant recours à un dispositif de signature électronique.

La liste des fonctionnalités offertes par Sécur'Pass Pro est susceptible d'évolution. Le Client en est informé via l'Application mobile ou via la documentation s'y rapportant.

Sécur'Pass Pro complète ou se substitue, le cas échéant, aux autres modes d'authentification.

L'enrôlement à Sécur'Pass Pro est effectué par toute Personne habilitée par la saisie de certains numéros aléatoires de sa carte bancaire ou de sa carte Sécur'Accès en cours de validité et active, émise par la Banque, ou à défaut, de son adresse de courrier électronique enregistrée par la Banque. L'enrôlement peut se faire aussi par une demande formulée auprès d'un conseiller en agence. La Personne habilitée doit posséder un appareil compatible (smartphone, tablette) pour télécharger l'Application mobile et un numéro de téléphone mobile préalablement déclaré à la Banque en tant que numéro de téléphone sécurisé. Afin d'utiliser Sécur'Pass Pro, la Personne habilitée doit également activer le service à partir de son Espace de banque à distance accessible depuis l'Application mobile. L'activation de Sécur'Pass Pro nécessite la saisie par la Personne habilitée d'un code temporaire reçu sur le numéro de téléphone communiqué ainsi que d'un code Sécur'Pass Pro qu'il a choisi.

Le changement d'appareil compatible (smartphone, tablette) initialement enregistré et/ou la réinstallation de l'Application mobile de la Banque nécessite l'enrôlement du nouvel appareil ou un nouvel enrôlement à Secur'Pass Pro.

Le choix, l'enregistrement, la modification, la réinitialisation et la conservation du code Sécur'Pass Pro sont de la responsabilité la Personne habilitée. Il lui appartient notamment de veiller à le conserver strictement secret, au même titre que l'ensemble des identifiant/mot de passe liés à son Espace de banque à distance ou à ses moyens de paiement. La Banque n'a aucun accès à ce code Sécur'Pass Pro.

Il est conseillé la Personne habilitée de changer son code Sécur'Pass Pro fréquemment, de ne pas choisir un code Sécur'Pass Pro simple aisément décelable par un tiers, et de ne pas choisir un code Sécur'Pass Pro identique à celui qu'il utiliserait déjà par ailleurs, par exemple, le code PIN associé à son smartphone ou à sa carte SIM, ou le code confidentiel lié à son accès à l'Espace de Banque à distance, ou le code associé à sa carte bancaire.

Lors de l'utilisation de Sécur'Pass Pro, la saisie du code Sécur'Pass Pro pourra éventuellement être effectuée par la Personne habilitée en utilisant la fonction biométrique de son appareil compatible (smartphone, tablette) si disponible.

La Personne habilitée a la possibilité de supprimer le dispositif Sécur'Pass Pro à tout moment. En cas de cession de son appareil compatible (smartphone, tablette), il lui appartient de veiller à la désactivation de Sécur'Pass Pro et à la désinstallation préalable de l'Application mobile.

La suppression de Sécur'Pass Pro est susceptible d'empêcher l'accès à certains services nécessitant le recours à une authentification forte, ou d'entraîner l'application d'exigences ou de délais complémentaires pour la réalisation de certaines opérations.

Pour pouvoir à nouveau accéder au dispositif Sécur'Pass Pro, la Personne habilitée devra procéder à un nouvel enrôlement.

La suspension ou la fermeture de l'accès à Sécur'Pass Pro pour quelque raison que ce soit, à l'initiative la Personne habilitée ou de la Banque, entraîne l'impossibilité d'utiliser le dispositif Sécur'Pass Pro et les fonctionnalités liées.

F) SERVICE DE SIGNATURE ÉLECTRONIQUE

L'utilisation du service « Signature électronique » est liée à la détention d'un dispositif d'Authentification forte. Dans le cadre du processus de Signature électronique par un dispositif d'Authentification forte, celui-ci reprend les fonctions d'Authentification

et de consentement de la signature auxquels est ajouté un procédé fiable de signature « à usage unique ou à la volée », garantissant le lien entre la Signature électronique et l'acte auquel elle s'attache. Ainsi, dans le cas où le Client transmet un ordre de paiement par l'intermédiaire de CE net (service CE net Remises ou protocole), il devra nécessairement apposer sa « Signature électronique » par l'intermédiaire du service Parafeur du service Signature électronique des ordres.

Les personnes autorisées par le Client à confirmer des ordres pour le compte de ce dernier par un dispositif d'Authentification forte sont indiquées en annexes des Conditions Particulières.

Il est précisé que ces autorisations valent délégation de pouvoirs spécifiquement applicables à la présente Convention quels que soient les pouvoirs communiqués par ailleurs, la Banque n'ayant pas d'autres contrôles à effectuer que le respect des délégations indiquées en annexes des Conditions Particulières.

G) MODALITÉS ET CONDITIONS D'ACCÈS AU SERVICE DE BANQUE À DISTANCE DEPUIS UN SERVICE EN LIGNE FOURNI PAR UNE ENTREPRISE TIERCE ET AUTORISATION DE PARTAGE DE DONNÉES

- Conditions d'accès

Sous réserve de disponibilité, la Banque permet au Client d'accéder à certaines fonctionnalités/opérations (notamment réalisation de virements unitaires ou groupés, ajout d'un bénéficiaire de virement, consultation de solde...) depuis un autre service en ligne (site internet / application, logiciel), ci-après dénommé « espace tiers », fourni par une entreprise tierce.

Le Client peut en bénéficier sous réserve des conditions suivantes :

- Le Client doit avoir souscrit un abonnement de banque à distance incluant ce nouveau canal d'échanges avec sa Banque à partir d'un service en ligne fourni par l'entreprise tierce, ce canal d'échanges ayant été mis en place préalablement entre la Banque et l'entreprise tierce ;
- Le Client a souscrit auprès de cette entreprise tierce le service en ligne de cette dernière et il doit également avoir donné son autorisation à l'entreprise tierce de recevoir de la Banque et de transmettre à la Banque ses données personnelles et non personnelles dans le cadre des opérations effectuées sur la banque à distance à partir de l'espace tiers ;
- Le Client a donné son autorisation à la Banque de partager ses données personnelles et non personnelles avec l'entreprise tierce dans le cadre des opérations effectuées sur la Banque à distance à partir de l'espace tiers. Par cette autorisation, le Client active le canal d'échanges avec l'entreprise tierce ;
- En présence de Personnes habilitées à effectuer des opérations dans son Espace de banque à distance, le Client reconnaît que ces derniers pourront autoriser ce partage de données personnelles et non personnelles et activer ce canal d'échanges avec la Banque depuis cet espace tiers pour effectuer des opérations dans le même périmètre qui leur a été imparti.

- Modalités d'accès

Depuis cet espace tiers, le Client / la Personne habilitée a la possibilité d'être redirigé vers une page de la Banque, où il doit s'authentifier avec ses éléments habituels de connexion à l'Espace de banque à distance. Lors de la première utilisation de ce nouveau canal d'échanges avec la Banque, le Client / la Personne habilitée doit autoriser le partage des données personnelles et non personnelles précitées pour activer ce canal d'échanges. Une fois cette étape réalisée, le Client est informé que la Banque peut communiquer à l'entreprise tierce des données personnelles et non personnelles liées aux opérations demandées par le Client / la Personne habilitée. Le Client / la Personne habilitée est informé des catégories d'informations communiquées à l'entreprise tierce, lors de son activation du canal d'échanges.

- Responsabilités

Il appartient au Client dans le cadre de sa relation contractuelle avec l'entreprise tierce de s'assurer que celle-ci n'utilise pas les données partagées pour une finalité autre que de permettre au Client de communiquer avec sa Banque à partir de son espace tiers/service en ligne.

La Banque n'est pas responsable des dysfonctionnements ou de la sécurité du service en ligne de l'entreprise tierce.

La Banque est responsable de la transmission à l'entreprise tierce des données demandées par le Client à partir de son espace tiers et du traitement des données reçues du Client par le biais de son espace tiers.

La Banque n'est pas responsable de la fréquence de la mise à jour par l'entreprise tierce des informations restituées dans l'espace tiers.

5.2 - Obligation des parties

5.2.1 - Obligations du Client

Le Client est responsable de l'équipement en dispositif d'Authentification forte de chacun de ses Utilisateurs, pour l'accès à CE net et, le cas échéant, pour la réalisation des virements et des Opérations sensibles.

Le Client/l'Utilisateur doit utiliser ses éléments d'identification et les dispositifs d'Authentification forte mis en place par la Banque chaque fois qu'il en reçoit l'instruction, sous peine d'engager sa responsabilité.

Toute personne qui en fera l'utilisation sera donc réputée autorisée par le Client et toutes les opérations seront réputées faites par lui. La Banque ne peut pas être tenue pour responsable en cas d'usage frauduleux ou abusif.

Dès qu'il reçoit un Instrument de paiement, le Client prend toute mesure raisonnable pour préserver la sécurité de ses Données de sécurité personnalisées qui sont placées sous sa garde. Il utilise son Instrument de paiement conformément aux conditions régissant sa délivrance et son utilisation et définies ci-après par Service.

5.2.2 - Obligations de la Banque

Lorsqu'elle délivre à un Client un Instrument de paiement, la Banque s'assure que les Données de sécurité personnalisées de cet Instrument ne sont pas accessibles à d'autres personnes que le Client et/ou l'(les) Utilisateur(s) autorisé(s) à utiliser cet Instrument, sauf si le Client/l'Utilisateur ne respectent pas les recommandations et obligations à leur charge.

Elle s'abstient d'envoyer tout Instrument de paiement non sollicité, sauf si un Instrument déjà donné doit être remplacé.

La Banque informera le Client, de façon sécurisée, en cas de soupçon de fraude, de fraude avérée ou de menaces pour la sécurité survenant sur le service CE net.

5.3 - Recommandations spécifiques relatives au Service CE net

Dans le souci de protéger la confidentialité des données bancaires du Client, la Banque, en particulier dans le cadre des règles d'usage d'internet, invite le Client à prendre toute disposition utile, notamment en effaçant, dès la fin de la consultation, les traces de sa navigation et en interdisant l'accès aux tiers non autorisés dans l'hypothèse de leur téléchargement vers un logiciel de gestion.

De façon générale, la Banque rappelle au Client qu'il lui appartient de protéger les données et/ou les logiciels stockés ou chargés, et/ou l'équipement informatique utilisé, de la contamination par des virus ou de tentatives d'intrusion, quelles qu'elles soient.

Le Client est tenu de sécuriser son ordinateur, sa tablette ou son téléphone mobile, au moyen de solutions de sécurité de son choix (verrouillage du téléphone, logiciel anti-virus et anti-espion, Pare-feu ...) et de maintenir ces dispositifs à jour en permanence.

Le Client est ainsi invité à prendre connaissance des mesures à mettre en œuvre afin de sécuriser ses connexions Internet en consultant la page « Sécurité » disponible sur le site Internet de la Banque (www.caisse-epargne.fr).

Dès lors que le Client autorise l'accès en ligne à son compte par un prestataire de service d'initiation de paiement (virements) ou d'information sur les comptes (service d'agrégation de comptes), ce prestataire doit disposer de l'agrément délivré par l'autorité compétente d'un Etat membre de l'Union Européenne ou être inscrit sur le registre tenu par cette autorité, conformément à la règlementation en vigueur. Le Client est tenu de vérifier que ce prestataire dispose de cet agrément ou est inscrit sur le registre concerné. Le Client peut être tenu de communiquer à ce prestataire, sous sa responsabilité, tout ou partie de ses éléments d'identification et d'authentification pour l'accès à CE net.

L'initiation d'opérations de paiement (virements) par ce prestataire, pour le compte du Client, s'effectuera selon les mêmes modalités et conditions d'authentification que si le Client réalisait directement ces opérations par l'intermédiaire de CE net. Toutefois, le cas échéant, l'initiation d'un virement unitaire par ce prestataire pourra être réalisée, par exception, sans inscription préalable du bénéficiaire par le Client sur la liste de ses bénéficiaires de virements.

ARTICLE 6 - OPPOSITION À L'UTILISATION DES SERVICES EN LIGNE DE CE NET

Le Client s'engage à se rendre immédiatement à son Agence ou à avertir immédiatement la Banque par lettre recommandée avec demande d'avis de réception, ou par tous autres moyens confirmés par lettre recommandée avec demande d'avis de réception, dès qu'il considère que la confidentialité de l'accès au Service n'est plus assurée pour quelque motif que ce soit.

6.1 - Opposition (blocage) à l'accès au Service consécutive à la perte ou vol des éléments d'identification et/ou d'Authenfication forte

Dès qu'ils ont connaissance de la perte, du vol, du détournement ou de l'utilisation frauduleuse des éléments d'identification et/ou d'Authentification forte personnels d'une Personne habilitée, le Client et/ou l'Utilisateur Principal doivent immédiatement en informer par tous moyens la Banque qui bloquera l'accès aux Services en ligne de CE net.

L'opposition devra être immédiatement confirmée par courrier recommandé avec demande d'avis de réception ou directement auprès de la Banque. En cas de contestation, la date de réception de l'écrit fera foi entre les parties.

Les conséquences d'une absence d'opposition sont précisées à l'article 15.4.

6.2 - Opposition à une carte de paiement ou à une carte Sécur@ccès utilisée dans le cadre de SOL par lecteur CAP

Dès connaissance de la perte, du vol ou d'une utilisation frauduleuse d'une carte Sécur@ccès, ou d'une carte de paiement, le Client, son représentant légal ou le porteur devra immédiatement faire procéder au blocage de cette dernière et confirmer par déclaration écrite auprès de la Banque ayant délivré la carte.

Le Client est invité à se référer, pour les conditions d'opposition aux cartes délivrées par la Banque et utilisables dans le cadre du Service, au contrat SOL par Lecteur CAP ou au contrat porteur carte.

La Banque ne saurait être tenue pour responsable des opérations effectuées dans le cadre du Service avec une carte délivrée par la Banque à défaut d'opposition dans les conditions contractuellement prévues.

6.3 - Révocation du Certificat électronique utilisé dans le cadre des Services en ligne de CE net

Dès qu'ils ont connaissance de la perte, du vol, du détournement ou de toute utilisation frauduleuse d'un Certificat électronique, le Client, ou son représentant légal, ou le mandataire de certification, ou encore le porteur du Certificat, doivent révoquer le Certificat électronique auprès de l'Autorité de Certification dans les conditions indiquées au contrat relatif au Certificat électronique souscrit par ailleurs par le Client, aux fins de blocage de ce dernier.

Le Client et/ou le porteur du Certificat en informe sans tarder et par tous moyens la Banque afin de bloquer l'utilisation du Certificat sur le Service.

La personne, dont le Certificat électronique est révoqué, ne peut plus alors s'authentifier et utiliser la fonction de Signature électronique de son Certificat notamment pour accéder aux Opérations sensibles proposées en ligne dans le cadre de CE net.

Toutes les opérations effectuées dans le cadre du Service à l'aide du Certificat électronique par une personne habilitée, avant publication par l'Autorité de certification, sont présumées émaner de ce dernier.

ARTICLE 7 - CONDITIONS D'EXÉCUTION DES OPÉRATIONS ET ORDRES DE PAIEMENT DÉPOSÉS VIA CE NET, TRANSMIS VIA UN TIERS INITIATEUR DE PAIEMENT (API), OU TRANSMIS VIA UN PROTOCOLE DE COMMUNICATION BANCAIRES EDI

Les ordres de paiement et les opérations qui découlent de CE net sont soumis aux conditions de traitement habituelles en vigueur à la Banque, à la date de l'opération et objet de la convention de compte courant régularisée par acte séparé par le Client ou de toutes autres conventions existantes liées à des services spécifiques signées par le Client, ainsi que le cas échéant par les conventions/contrats liés aux différents protocoles utilisés (EBICS, SWIFTNET), sauf conditions spécifiques prévues dans les conditions particulières de la convention de compte courant, et/ou dans les Conditions Particulières du Contrat.

Ainsi, le Client doit vérifier la bonne exécution de ses ordres, notamment lorsqu'ils sont destinés au paiement de sommes dues à date fixe.

7.1 - Dispositions applicables aux remises d'ordres de virements SEPA

Concernant les remises d'ordres de virements SEPA (Classique, Jour, Spécial, Instantané) et les prélèvements SEPA (Core ou Interentreprise), le Client pourra choisir, sous réserve de disponibilité, le mode de comptabilisation de la remise sur le compte donneur d'ordres :

- Comptabilisation Nette : la remise d'ordres traitée sera comptabilisée, sur le compte du Client donneur d'ordre, de la somme totale des ordres transmis sous déduction des ordres écartés selon les contrôles de faisabilité effectués par les systèmes de traitement de la Banque.
- Comptabilisation Brute : la remise d'ordres sera comptabilisée sur le compte du Client donneur d'ordre de la somme totale des ordres transmis. Les ordres qui auront été écartés et non échangés, selon les contrôles de la Banque, seront comptabilisés sur le compte du Client donneur d'ordre dans le sens inverse de la remise des ordres.

La Banque peut être amenée à soumettre les remises d'ordres de virements ou de prélèvements à des limites de plafonds par client. Ces limites peuvent être par ordre unitaire, cumul journalier et cumul mensuel. Dans le cas de dépassement de l'un de ces plafonds, la remise ne sera pas traitée ce dont le Client sera informé.

Fonctionnalité d'anonymisation des informations relatives aux virements de salaires, dans les relevés mis à la disposition du client (sous réserve de disponibilité) :

Pour les fichiers de remises d'ordres SEPA et s'agissant de règlement de virements de salaires, le Client pourra demande d'opter pour la fonctionnalité d'anonymisation des informations relatives aux virements de salaires au niveau des relevés mis à la disposition du Client ou en consultation sur CE net.

Cette fonctionnalité est disponible sur les remises d'ordres virement SEPA (Classique, Jour, Spécial), sous réserve que le Client renseigne à « SALA » la balise « category purpose » dans son fichier d'ordres transmis préalablement (<CtgyPurp>SALA</CtgyPurp>, au niveau lot - Payment Information - de la remise). La Banque anonymisera l'ensemble des informations (Nom, Prénom, Adresse du bénéficiaire).

Par ailleurs, dans le cas où le Client a fait le choix d'une comptabilisation unitaire, l'anonymisation sera aussi appliquée sur le relevé de compte des ordres transmis.

Vérification du bénéficiaire - Virements SEPA déposés sous forme de fichier (Classique, Jour, Spécial, Instantané) (service permettant de renforcer la sécurité des virements et de réduire les risques d'erreurs et de fraudes) **:**

- Principes généraux

Conformément au Règlement (UE) 2024/886 du 13 mars 2024, ce service permet au Client de demander à la Banque d'effectuer une vérification des bénéficiaires de virements SEPA classiques et instantanés, auprès de leur Prestataire de Service de Paiement (PSP). Cette vérification porte sur la concordance entre l'IBAN et le nom du bénéficiaire de virement SEPA. Ce service est fourni au Client à titre gratuit.

- Réalisation de la vérification

Lors de la remise de chaque fichier d'ordres de virements SEPA sous une forme groupée, le Client peut choisir :
- de soumettre ce fichier à la vérification des bénéficiaires ou,
- de bénéficier du service de « Vérification à la demande » ou,
- de renoncer à la vérification des bénéficiaires.

- Renonciation au service de vérification du bénéficiaire

Lors du dépôt de chaque fichier de remise d'ordres de virements SEPA, le Client peut renoncer au service de vérification du bénéficiaire pour le fichier concerné. En renonçant à ce service, le Client est informé que les virements pourraient être crédités sur le compte d'un autre bénéficiaire que celui auquel le Client souhaite transmettre les fonds. Le Client peut décider, à tout moment, de bénéficier à nouveau de ce service, lors du dépôt d'un nouveau fichier de remise d'ordres de virement.

- « Vérification à la demande »

Dans le cas où le Client souhaite que cette vérification des bénéficiaires soit réalisée pour ce fichier, il lui est proposé de demander uniquement la vérification des bénéficiaires, sans exécution des virements, dans le cadre du service « Vérification à la demande », s'il a préalablement souscrit à ce service dans les Conditions Particulières du Contrat.

Après consultation des résultats de la vérification, le Client transmettra un fichier d'ordres de virement pour exécution qui ne fera pas l'objet d'une vérification des bénéficiaires.

Ce service ne peut être utilisé à d'autres fins que la vérification des bénéficiaires au préalable d'une opération de virement SEPA. Le Client s'engage à ne pas utiliser le service de manière à le détourner de sa finalité.

- Résultats de la vérification

Le résultat de la vérification des bénéficiaires est mis à disposition du Client par la Banque, dans le suivi des remises, dans les Relevés et dans le Parapheur, avant signature des ordres. Ce rapport détaille le résultat de la vérification pour chaque bénéficiaire :
- Concordance : le nom associé à l'IBAN correspond au nom du bénéficiaire que le Client a renseigné.
- Concordance partielle : le nom associé à l'IBAN ne correspond pas exactement au nom du bénéficiaire que le Client a renseigné. La Banque communique alors au Client le nom du bénéficiaire associé à l'IBAN qu'il a fourni.
- Non concordance : le nom associé à l'IBAN ne correspond pas au nom du bénéficiaire que le Client a renseigné. La Banque ne lui donne aucune information sur le bénéficiaire.
- Vérification impossible : la concordance entre l'IBAN et le nom du bénéficiaire que le Client a renseigné n'a pas pu être vérifiée. Le Client est également informé si le compte du bénéficiaire est clôturé.

Ce résultat n'est valable qu'au moment de la mise à disposition du rapport par la Banque au Client, et ne saurait en aucun cas prévaloir pour l'avenir.

Une validation des bénéficiaires par le Client sera nécessaire en cas d'anomalie de concordance afin de permettre à la remise de virements de remonter dans le Parapheur en vue de la signature des ordres.

En cas de concordance partielle et de non-concordance, le Client est informé que l'autorisation du virement pourrait conduire à ce que les fonds soient virés sur le compte d'un autre bénéficiaire que celui auquel le Client souhaite transmettre les fonds.

Si, malgré les alertes, le Client autorise le virement, la Banque l'informe :
- Que le virement est considéré comme exécuté au profit du bon bénéficiaire ;
- Qu'elle ne peut pas être tenue responsable de l'exécution de ce virement au profit d'un mauvais bénéficiaire ;
- Qu'il n'a pas droit au remboursement de ce virement pour opération mal exécutée.

7.2 - Dispositions applicables aux LCR/BOR

Le Client peut remettre des LCR et des BOR à l'encaissement, à l'escompte, à titre de garantie d'un crédit ou d'une avance de trésorerie. La confirmation des ordres est réalisée par Signature électronique et de façon exceptionnelle par télécopie.

Lorsque le Client remet des LCR et des BOR à l'escompte, ou à titre de garantie d'un crédit ou d'une avance, il doit avoir préalablement signé une convention-cadre de cession de créances professionnelles ayant pour objet de préciser les modalités d'application de la loi dans ses rapports avec la Banque. Un bordereau de cession de créances (Dailly) doit être corrélativement joint à cette remise.

En tout état de cause, quelle que soit l'option choisie, chaque remise de LCR et/ou de BOR confirmée par Signature électronique doit être accompagnée d'un bordereau de cession de créances Dailly établi à l'ordre de la Banque conformément à la convention cadre de cession de créances. Le bordereau de cession de créances Dailly sera transmis soit par télécopie à la Banque et ce concomitamment au dépôt de la remise, soit confirmé sur CE net par Signature électronique. Dans ce dernier cas, le Client, à la suite de son dépôt de remise de LCR ou BOR, devra confirmer par Signature électronique le bordereau de cession en format PDF, généré à partir des informations contenues dans la remise transmise par le Client.

7.3 - Service de Protection (CE Net Remises et CE Net EDI)

7.3.1 - Contrôle de liste sur pays approuvés

Ce contrôle permet de vérifier la cohérence entre le code pays du destinataire du flux télétransmis et la liste des codes pays destinataires approuvés par le Client. Une limite de montant peut être définie par opération. En cas de divergence l'opération est rejetée.

7.3.2 - Contrôle de liste des Comptes destinataires approuvés

Ce contrôle permet de vérifier la cohérence entre les destinataires du flux télétransmis et la liste des Comptes destinataires approuvés par le Client et par type de remise. En cas de divergence l'opération est rejetée.

ARTICLE 8 - MODALITÉS D'AUTORISATION DES ORDRES DE PAIEMENT

Une opération ou une série d'opérations de paiement est autorisée si le donneur d'ordre a donné son consentement à son exécution ou à l'exécution de la série d'opérations.

8.1 - Transfert de fichiers à l'aide des protocoles EBICS, Pe SIT hors SIT ou le service CE net Remises

Le transfert de fichiers doit faire l'objet d'une confirmation de l'ordre.

Cette confirmation prend la forme d'une Signature électronique, conformément aux habilitations définies en annexes des Conditions Particulières du Contrat ou des protocoles de communication concernés le cas échéant.

Il est précisé que le Client donne mandat à la Banque de procéder à l'exécution de tous les ordres de paiement dont la Signature électronique sera effectuée à l'aide d'un Certificat en cours de validité ou d'un Lecteur CAP selon les modalités décrites à l'article 5.

A titre exceptionnel, en solution de contournement, et avec l'accord de la Banque, la confirmation pourra être transmise par télécopie revêtue de la ou des signatures accréditées préalablement.

Sauf limites stipulées aux annexes relatives aux « habilitations de signature » et/ou aux conventions liées au protocole de communication le cas échéant, les Personnes habilitées par le Client, à remettre et/ou à signer les ordres sont réputées avoir tous pouvoirs. Elles sont donc réputées agir par délégation et sous l'entière responsabilité du Client.

La confirmation de l'ordre doit contenir le type d'opérations transmises, le numéro de compte Banque du donneur d'ordre, le nombre d'opérations, le montant global de la remise, la devise le cas échéant, et la date d'exécution souhaitée.

L'application de cette procédure par le Client vaut consentement de ce dernier à l'exécution de l'opération.

Par ailleurs, à défaut de dispositions contraires spécifiques, la Banque n'exécutera pas les instructions transmises par EDI et confirmées autrement que par Signature électronique, voire, dans les conditions visées ci-dessus, par télécopie notamment celles confirmées verbalement, par téléphone, ou par courriel.

De plus, il est précisé que la Banque est dégagée de toute responsabilité pour l'exécution, une seconde fois, de l'ordre transmis deux fois par le Client :

- par EDI avec confirmation,
- et par courrier ou par télécopie,

sans qu'il soit fait expressément mention qu'il s'agissait du même ordre.

Le fichier EDI transmis par le Client et sa confirmation, soit par Signature électronique sur CE net, soit par Signature électronique jointe au fichier, voire par télécopie, constitueront, sauf preuve contraire, le mode de preuve du contenu et de la transmission des instructions exécutées par la Banque ; ils engageront le Client dans les mêmes conditions et avec les mêmes effets juridiques qu'un écrit comportant une signature manuscrite.

8.2 - Transfert de fichier utilisant le service SWIFTNet FileAct ou SWIFTNet FIN sans signature jointe

Lorsque le Client a choisi aux Conditions Particulières de la convention relative aux protocoles bancaires de confirmer ses ordres par Signature électronique via CE net EDI, les dispositions prévues au Contrat sont applicables.

Lorsque le Client utilise SWIFTNet FileAct ou SWIFTNet FIN sans signature jointe et choisit aux Conditions Particulières de la convention relative aux protocoles bancaires de ne pas confirmer ses ordres par Signature électronique via CE net EDI, les dispositions suivantes sont applicables :

Dès lors que le Client est correctement identifié selon les modalités décrites à la convention SWIFTNet, signée par acte séparé, il est expressément convenu entre les parties que :
- la remise d'ordre est émise par le Client de façon certaine,
- cette Authentification vaut consentement du Client à l'exécution de l'opération.

Le Client prend alors l'entière responsabilité du processus d'émission des ordres à partir de sa station Swift internalisée ou gérée par un prestataire. Il est expressément convenu entre les parties, qu'aucune contestation d'un ordre de paiement émis à partir de son BIC ou le BIC du mandataire pour opération non autorisée ne sera donc admise. Cependant, en cas de déclaration par le Client de la perte ou du vol de l'accès sécurisé SWIFT, une telle contestation pourra être formulée par le Client, dans le cas où cette déclaration aura été faite préalablement à l'Identification du Client et adressée à SWIFT et à la Banque.

ARTICLE 9 - MODALITÉS DE CONFIRMATION DES FICHIERS DE REMISES D'ORDRES DÉPOSÉS VIA LE SERVICE OU TRANSMIS PAR UN PROTOCOLE DE COMMUNICATION BANCAIRE

Les fichiers de remises d'ordres transmises à l'aide des protocoles EBICS - Profil T (transport uniquement), Pe SIT, ou encore saisis ou déposés sur CE net doivent être confirmées par le Client, de façon disjointe par Sécur'Pass Pro, Lecteur CAP ou Certificat électronique en cours de validité. Seules les opérations valides seront proposées à la signature disjointe.

Concernant la confirmation des ordres par Certificat Electronique, celle-ci peut s'effectuer :
- soit de façon jointe au fichier conformément aux dispositions du protocole utilisé : EBICS – profil TS (Transport et Signature jointe) et SWIFTNet FileAct signé,
- soit de façon disjointe via CE net pour les ordres transmis par les protocoles EBICS – profil T (Transport uniquement), saisis ou déposés sur CE net. Seules les opérations valides seront proposées à la signature disjointe.

L'utilisation du Certificat électronique ou Lecteur Cap dans le cadre de la Signature électronique doit être conforme aux conditions décrites à l'article 5 ci-dessus.

Dans le cas contraire, la Banque ne pourra être tenue responsable de la signature par Certificat électronique d'un ordre non autorisé.

Le contenu du fichier doit être validé par le Client avant toute confirmation par Signature électronique.

A titre exceptionnel, en solution de contournement et avec l'accord de la Banque, le Client peut confirmer par télécopie ses saisies ou transferts d'ordres. Toutefois, cette procédure dégrade la sécurité des saisies ou transferts d'ordres et la Banque déconseille au Client d'utiliser ce moyen de confirmation. Dans tous les cas, le Client assumera toutes les conséquences qui résulteraient des risques inhérents aux confirmations par télécopie.

Pour chaque nature d'opérations, la confirmation doit parvenir à la Banque, au plus tard avant les échéances précisées aux Conditions Particulières du Contrat.

ARTICLE 10 - CONDITIONS D'UTILISATION ET DISPONIBILITÉ DU SERVICE

10.1 - Généralités

Le Service est accessible via le réseau Internet 24 heures sur 24 et 7 jours sur 7 sur tout type de supports (ordinateurs, tablettes, smartphones).

Le Service peut être suspendu pour assurer sa maintenance ou sa mise à jour ou pour des motifs non imputables à la Banque, notamment en cas de force majeure ou du fait de tiers tels que les opérateurs de réseaux de télécommunications.

Le Client sera informé par la Banque par tous moyens, des nécessaires périodes de maintenance programmée.

10.2 - Règlement des incidents

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

ARTICLE 11 - PREUVE DES OPÉRATIONS ET DÉLAI DE RÉCLAMATION

Les opérations effectuées par le Client par l'intermédiaire du Service et portées sur le relevé ou arrêté de compte qui lui est adressé, peuvent être contestées par ce dernier dans le délai et aux conditions indiquées dans la convention de compte courant ou, le cas échéant dans la/les conventions liés aux différents protocoles utilisés par le Client (EBICS, SWIFTNET) et signées par ce dernier.

11.1 - Enregistrements

La preuve des opérations effectuées dans CE net pourra être faite par toute forme d'enregistrements résultant des moyens de communication utilisés entre le Client, les Personnes habilitées et la Banque.

Plus particulièrement, la Banque met à disposition du Client un accusé de réception relatif aux échanges effectués :
- via les protocoles de communication bancaire, EBICS et service SWIFTNet FileAct ou SWIFTNet FIN,
- ou via CE net.

De convention expresse, les parties ne reconnaissent que les enregistrements effectués par la Banque, quel qu'en soit
- le support,
- le type ou le montant des opérations réalisées,
- le fichier EDI ou les remises d'ordres,
- la Signature électronique,
- l'accusé de réception,
- les notifications adressées par SWIFT lors de chaque échange,
- les enregistrements réalisés par SWIFT.

Ces enregistrements informatiques (notamment les logs d'échanges et les données reçues) ainsi que leur reproduction réalisée par la Banque, feront foi entre les parties sauf preuve contraire.

11.2 - Preuve du consentement du Client

De convention expresse, la Banque et le Client reconnaissent que :
- l'identification correcte du Client, associé à l'accusé de réception, leur permet de considérer les fichiers comme valablement déposés sur la plateforme informatique de la Banque,
- les fichiers informatiques étant transmis et confirmés par le Client en recourant à l'utilisation de certificats de transport ou de certificats d'Authentification ou de cartes paramètre, celui-ci est réputé en être l'auteur,
- les interrogations ou les ordres sont réputés émaner du Client dès lors qu'ils sont constitués, du numéro du Client, du numéro d'Utilisateur et du code confidentiel, et le cas échéant de l'utilisation d'un Certificat électronique ou d'un moyen d'Authentification forte. Ces éléments constituent une preuve du consentement des opérations sollicitées et/ou réalisées.

11.3 - Récapitulatif des transactions

La preuve des opérations effectuées pourra également être rapportée par tous moyens notamment par les récapitulatifs des transactions établis par les systèmes informatiques de la Banque.

ARTICLE 12 - INTÉGRITÉ, CONFIDENTIALITÉ DU SERVICE

La Banque assure une totale confidentialité des données saisies par le Client dans CE net.

La saisie d'ordres par le Client sera systématiquement chiffrée. Ce chiffrement au moyen d'une clé de cryptage permet d'assurer la confidentialité des échanges. Il appartient au Client de disposer des logiciels permettant ce niveau de protection.

ARTICLE 13 - MODIFICATION DES CONDITIONS PARTICULIÈRES ET DES CONDITIONS GÉNÉRALES DE CE NET

13.1 - Modification du fait de la Banque

La Banque aura la faculté de modifier les Conditions Générales et les Conditions Tarifaires du Service. A cet effet, la Banque communiquera le projet de modification par écrit (par exemple, lettre, mention sur le relevé de compte ou information dans son Espace de banque à distance) au Client, au plus tard un mois avant la date d'application envisagée.

La Banque et le Client conviennent que l'absence de contestation du Client dans ce délai vaut acceptation par ce dernier des modifications. En cas de refus du Client, ce dernier peut résilier sans frais, avant la date d'application des modifications, le Contrat. A défaut de résiliation dans ce délai, les modifications lui seront opposables.

Compte tenu de l'évolution nécessaire et régulière des moyens de sécurité, la Banque se voit expressément reconnaître par le Client, sans recours possible de ce dernier contre la Banque, la possibilité, à tout moment et à effet immédiat, de modifier de façon unilatérale les conditions d'authentification nécessaires à l'accès aux services, ou de supprimer certains dispositifs d'authentification moyennant une information du Client par tout moyen au choix de la Banque.

13.2 - Modifications imposées par des textes législatifs ou règlementaires

Les modifications de tout ou partie du Contrat qui seraient rendues nécessaires par des dispositions législatives ou réglementaires, seront applicables dès leur date d'entrée en vigueur, sans préavis ni information préalable.

ARTICLE 14 - TARIFICATION

La tarification varie selon le niveau d'offre souscrit conformément aux Conditions Tarifaires en vigueur.

Le coût de l'abonnement et la tarification liée aux fonctionnalités, services et opérations effectuées seront prélevés sur le (les) compte(s) mentionné(s) dans les Conditions Particulières.

La tarification pourra être révisée à tout moment. Le nouveau tarif sera porté à la connaissance du Client dans les conditions prévues par l'article 13.

Le Client supportera le coût des consommations téléphoniques ainsi que tout montant, redevance, abonnement ou taxes afférentes à l'abonnement téléphonique ou auprès du fournisseur d'accès internet.

14.1 - Coût de l'abonnement

La tarification du Service est composée d'un abonnement forfaitaire mensuel et/ou d'une tarification par service dont le montant est fixé dans les Conditions Tarifaires de la Banque ou aux Conditions Particulières.

14.2 - Tarification des opérations effectuées et des actes de gestion

Par ailleurs, le Client reconnaît avoir été informé que les services et/ou opérations et/ou actes de gestion sollicités et/ou effectués, notamment par l'intermédiaire de CE net, peuvent donner lieu à tarification conformément aux Conditions Tarifaires de la Banque, dont le Client reconnaît avoir pris connaissance et qui sont notamment disponibles dans les agences et sur le site Internet de la Banque.

ARTICLE 15 - RESPONSABILITÉS DE LA BANQUE ET DU CLIENT

15.1 - Responsabilité de la Banque

15.1.1 - Engagements de la Banque

La Banque s'engage à tout mettre en œuvre pour assurer le bon fonctionnement du Service, notamment la bonne exécution des ordres reçus et la confidentialité des informations communiquées.

D'une manière générale, la Banque ne pourra être tenue pour responsable que des dommages ayant pour cause unique son propre fait.

Au cas où la responsabilité de la Banque serait établie, seul le préjudice personnel, prévisible, matériel et direct du Client donnera lieu à réparation.

La Banque ne saurait être tenue pour responsable :

- en cas de non-respect par le Client ou tout Utilisateur des procédures d'utilisation de CE net, en cas de divulgation du ou des codes confidentiels (dont ceux générés par le dispositif d'Authentification forte) à une tierce personne, y compris à un prestataire de service d'initiation de paiement ou d'information sur les comptes, disposant d'un agrément ou d'un enregistrement prévu par les textes en vigueur,
- en cas d'utilisation, par une tierce personne, du Certificat électronique, du service SOL SMS, du service Sécur'Pass Pro, ou de l'Authentification fournie par le service de Sécurisation des Opérations en Ligne par Lecteur CAP (SOL par Lecteur CAP),
- lorsque les informations communiquées par le Client, y compris sur les Utilisateurs, lors de l'adhésion ou lors de l'utilisation de CE net s'avèrent inexactes ou incomplètes,
- en cas de connexion du Client ou de tout Utilisateur à un autre site que le Site légitime et sécurisé de la Banque,
- en cas d'interruption temporaire du Service pendant des périodes courtes pour des raisons techniques et en vue de réaliser des prestations de maintenance ou d'actualisation du Service ou de l'Application mobile de la Banque,

- en cas d'interruption des prestations pour des raisons résultant de la force majeure, du cas fortuit ou du fait d'un tiers,
- des conséquences résultant d'un défaut de sécurité (matériel ou logiciel, antivirus) du terminal de connexion (ordinateur, terminal mobile...) utilisé par le Client ou tout Utilisateur n'ayant pas détecté, notamment, l'intrusion d'un virus informatique.

Sont, notamment considérés comme cas de force majeure :
- Le défaut de fourniture de courant électrique,
- les interruptions de service consécutives au mauvais fonctionnement du matériel utilisé par le Client,
- la défaillance du transporteur d'information ou les incidents affectant les lignes et réseaux de transmission,
- les guerres, émeutes, grèves, incendie...

15.1.2 - Causes d'exemption de la responsabilité de la Banque
La responsabilité de la Banque ne saurait être engagée en raison des conséquences directes et indirectes liées aux mesures, quelles qu'elles soient, notamment gel des avoirs, qu'elle pourrait être amenée à prendre dans le cadre des obligations mises à sa charge par les pouvoirs publics, en particulier au titre de la lutte contre le blanchiment des capitaux et le financement du terrorisme. A ce titre, la Banque ne saurait être tenue pour responsable des retards d'exécution.

La Banque demeure étrangère à tout litige pouvant survenir entre le Client et son prestataire de service d'initiation de paiement ou d'information sur les comptes.

15.2 - Responsabilité du Client quant aux opérations effectuées par les Personnes habilitées dans CE net

Le Client s'engage notamment au respect des conditions d'utilisation du Service, et particulièrement au respect des instructions liées à la sécurité du Service définies dans les Conditions Générales et les Conditions Particulières.

Le Client dégage la Banque de toute responsabilité en cas, par exemple, d'un défaut de traitement d'un fichier en raison du non-respect des contraintes techniques du Service par le Client.

15.2.1 - Délégation responsabilité du Client
L'Utilisateur Principal, s'il n'est pas le Client lui-même, ainsi que les Administrateurs, sont considérés comme expressément habilités par le Client à l'effet de gérer les droits des personnes ayant accès au Service comme indiqué à l'article 3 ci-dessus.

Toute Personne habilitée sera réputée agir par délégation et sous l'entière responsabilité du Client.

Le Client reste tenu des conséquences relatives à la conservation et à la préservation de la confidentialité des codes dédiés au Service, par lui-même et par les Personnes habilitées.

Le Client est seul responsable vis-à-vis de la Banque du choix des Personnes habilitées et des opérations passées par ces dernières, notamment en cas de fraude ou d'abus de confiance. La Banque n'est tenue à cet égard à aucun contrôle ou vigilance particulière, et n'est pas tenue des conséquences financières qui résulteraient d'une mauvaise utilisation ou délivrance des codes susvisés.

15.2.2 - Responsabilité du Client sur les ordres saisis et déposés
Les ordres saisis ou déposés sont sous la responsabilité exclusive du Client. La Banque n'est tenue à cet égard à aucun contrôle ou vigilance particuliers. La Banque n'ayant pas d'autres contrôles à effectuer que le respect des habilitations indiquées dans les Conditions Particulières. A ce titre, la Banque n'est pas tenue responsable des conséquences financières qui résulteraient d'une mauvaise indication des montants et/ou des comptes de destinataires des ordres.

La Banque décline toute responsabilité pour les conséquences quelconques qui pourraient résulter des retards, des erreurs ou des omissions dans la transmission ou le contenu des messages adressés par le Client, ainsi que de leur mauvaise interprétation, pour autant que ces retards, erreurs, montages ou omissions ne soient pas imputables à la Banque.

15.3 - Cas d'une suppression de Personnes habilitées ou d'un changement de rôle

En cas de suppression d'une Personne habilitée ou d'un changement de rôle, le Client reste tenu des opérations effectuées par cette dernière et ce, antérieurement à la modification des Conditions Particulières.

15.4 - Cas particulier des opérations non autorisées consécutives à la perte ou au vol

Les parties conviennent expressément de déroger à l'article L.133-19 du code monétaire et financier de la façon suivante.

En cas d'opération de paiement non autorisée consécutive à la perte ou au vol d'un Instrument de Paiement et/ou de ses Données de sécurité personnalisées, il est précisé que :
- avant l'information prévue à l'article 6 ci-dessus, le payeur supporte toutes les pertes liées à l'utilisation de cet Instrument ou de ses Données de sécurité personnalisées. Toutefois, le Client ne supporte aucune conséquence financière :
  - en cas de perte ou de vol des Données de sécurité personnalisées ne pouvant être détectée par le Client avant le paiement du Client,

- en cas de perte de ces Données de sécurité personnalisées due à des actes ou à une carence d'un salarié, agent ou d'une succursale de la Banque ou d'une entité vers laquelle ses activités ont été externalisées,
- lorsque cette opération a été effectuée sans utilisation des Données de sécurité personnalisées,
- lorsque l'opération non autorisée a été effectuée en détournant, à l'insu du Client, les Données de sécurité personnalisées liées à l'Instrument de paiement ou si elle résulte d'une contrefaçon de l'Instrument de paiement alors qu'au moment de l'opération de paiement non autorisée, il était en possession de son Instrument.

• à compter de l'information prévue à l'article 6, le payeur ne supporte aucune conséquence financière résultant de l'utilisation de l'Instrument de paiement ou de l'utilisation détournée des Données de sécurité personnalisées qui lui sont liées sauf agissement frauduleux de sa part. Dans le cadre d'une utilisation de Certificat électronique, cette disposition ne s'applique qu'à compter de la publication par l'Autorité de certification de la révocation du Certificat. Par conséquent, la Banque ne pourra pas être tenue responsable de la signature d'un ordre réalisée à l'aide d'un Certificat dont la révocation n'est pas encore publiée.

Le Client payeur supporte toutes les pertes occasionnées par des opérations de paiement non autorisées, si ces pertes résultent d'un agissement frauduleux de sa part ou s'il n'a pas satisfait, intentionnellement ou par négligence grave, aux obligations visées à l'article 6 ci-dessus.

Dans le cadre du présent contrat, l'indemnisation due par la partie responsable sera limitée aux seules pertes directes en capital et en trésorerie, subies par l'autre partie.

ARTICLE 16 - SECRET PROFESSIONNEL

La Banque est tenue au secret professionnel, conformément aux dispositions du Code monétaire et financier en vigueur.

Cependant, le secret est levé en vertu de dispositions légales, réglementaires, ou de conventions conclues par la France à des fins fiscales, notamment à l'égard de l'administration fiscale et des douanes, de la Banque de France, des organismes de sécurité sociale, de l'Autorité de contrôle prudentiel et de résolution, de l'autorité judiciaire agissant dans le cadre d'une procédure pénale, ainsi que dans le cadre d'une procédure civile, ou lorsqu'un texte spécifique le prévoit expressément.

La Banque peut partager avec les personnes, ci-après visées, avec lesquelles elle négocie, conclut ou exécute notamment les opérations, ci-après énoncées, des informations confidentielles concernant le Client, dès lors que ces informations sont nécessaires à celles-ci, ce que le Client accepte expressément :

- avec les entreprises qui assurent la mise en place ou la gestion d'un produit ou d'un service souscrit par le Client aux seules fins d'exécution des obligations contractuelles vis-à-vis de la Banque et du Client et plus généralement - avec des tiers (prestataires, sous-traitants, ...) en vue de leur confier des fonctions opérationnelles (par exemple : l'alerte sur l'utilisation de l'autorisation de découvert, le recours à des solutions de paiement mobile, la gestion des cartes bancaires, ou la fabrication de chéquiers) ;
- avec les entreprises qui assurent ou garantissent les crédits de ses clients (entreprises d'assurances, sociétés de caution mutuelle, par exemple) ;
- avec les entreprises qui octroient des crédits à ses clients ;
- avec des entreprises de recouvrement ;
- des entités appartenant au même groupe que la Banque (BPCE, Caisses d'Epargne, Oney Bank, BPCE Assurances, BPCE Financement, BPCE Lease et plus généralement toute autre entité du Groupe BPCE), pour l'étude ou l'élaboration de tous types de contrats ou d'opérations concernant ses clients ;
- des entreprises tierces en cas de cession de créances.

Les personnes recevant des informations couvertes par le secret professionnel, qui leur ont été fournies pour les besoins d'une des opérations ci-dessus énoncées, doivent les conserver confidentielles, que l'opération susvisée aboutisse ou non. Toutefois, dans l'hypothèse où l'opération susvisée aboutit, ces personnes peuvent à leur tour communiquer les informations couvertes par le secret professionnel.

Le Client victime d'une fraude ou d'une tentative de fraude autorise expressément la Banque à communiquer aux autorités policières et judiciaires son nom, son adresse, ainsi que son identifiant et plus généralement toute information nécessaire à la dénonciation de faits constitutifs d'un délit et ce afin d'apporter son concours à la justice dans le cadre de la lutte contre la fraude.

Il est précisé que les informations visées ci-dessus couvertes par le secret professionnel sont communiquées aux autorités judiciaires et policières dans le cadre étroit d'une enquête elle-même couverte par le secret visé à l'article 11 du Code de procédure pénale.

Le Client autorise expressément et dès à présent la Banque à communiquer et partager les données le concernant ainsi que leurs mises à jour :

- à BPCE S.A. agissant en qualité d'organe central du Groupe BPCE pour l'exercice des compétences prévues par le Code monétaire et financier afin que celui-ci puisse satisfaire aux différentes missions qui lui sont dévolues, au bénéfice de la Banque et du Groupe, notamment en matière de déclarations prudentielles auprès de toute autorité de régulation compétente ;

- à toute entité du Groupe BPCE en vue de la présentation au Client des produits ou services gérés par ces entités ;
- aux entités du Groupe BPCE avec lesquelles le Client est ou entre en relation contractuelle aux fins d'actualisation des données collectées par ces entités, y compris des informations relatives à son statut fiscal ;
- aux entités du Groupe BPCE en cas de mise en commun de moyens techniques, notamment informatiques ainsi que de gestion de gouvernance des données, pour le compte de la Banque. A cet effet, les informations personnelles concernant le Client couvertes par le secret bancaire pourront être pseudonymisées à des fins de recherches et de création de modèle statistique ;
- aux partenaires de la Banque, pour permettre au Client de bénéficier des avantages du partenariat auquel il adhère, le cas échéant, et ce dans le cadre exclusif des accords de partenariat ;
- aux sous-traitants et prestataires pour les seuls besoins des prestations à réaliser pour la Banque et notamment la fourniture des produits bancaires et financiers ou la réalisation d'enquêtes ou de statistiques.

Le Client autorise expressément la Banque à transmettre aux entités du Groupe BPCE auprès desquelles il a souscrit des produits ou services les informations actualisées sur son état civil, sa situation familiale, patrimoniale et financière, le fonctionnement de son compte ainsi que la note qui lui est attribuée pour l'application de la réglementation bancaire, afin de permettre l'étude de son dossier, l'utilisation des produits ou services souscrits, ou de leur recouvrement.

ARTICLE 17 - LUTTE CONTRE LE BLANCHIMENT DES CAPITAUX ET LE FINANCEMENT DU TERRORISME - RESPECT DES SANCTIONS INTERNATIONALES

17.1 - Lutte contre le blanchiment des capitaux et le financement du terrorisme

En application des dispositions légales et règlementaires prévues par le Code Monétaire et Financier (Livre V, Titre VI, Chapitre premier, partie législative et partie règlementaire), la Banque est tenue, dans le cadre de ses obligations relatives à la lutte contre le blanchiment des capitaux et le financement du terrorisme, de procéder à l'identification et à la vérification de l'identité des clients et le cas échéant, de leurs bénéficiaires effectifs. Un bénéficiaire effectif s'entend de la personne physique, soit qui contrôle, directement ou indirectement, une personne morale, soit pour laquelle une transaction est exécutée ou une activité réalisée.

Au même titre, la Banque est tenue de recueillir des informations relatives à l'objet et à la nature de la relation d'affaires, d'actualiser ces informations et d'exercer une vigilance constante à l'égard des opérations réalisées par sa clientèle pendant toute la durée de la relation d'affaires (montant et nature des opérations, provenance et destination des fonds, suivi de la situation professionnelle, économique et financière du Client ...).

A cette fin, le Client s'engage à fournir, à première demande, à la Banque ces informations et les justificatifs afférents. A défaut de les fournir ou en cas de fourniture d'informations erronées par le Client, la Banque pourra être conduite, en vertu des dispositions légales et réglementaires précitées, à résilier les conventions conclues avec le Client.

La Banque est également tenue d''appliquer des mesures de vigilance complémentaires à l''égard de ses clients Personnes Politiquement Exposées (P.P.E.) définies aux articles L. 561-10 1° et R. 561-18 du Code Monétaire et Financier, et par les dispositions de l''arrêté ministériel du 17 mars 2023 fixant en application dudit article R. 561-18 la liste des fonctions françaises concernées, ou à l'égard de ses clients personnes morales dont les bénéficiaires effectifs seraient dans cette situation. A ce titre, la Banque peut procéder, selon le cas, à un recueil d'informations auprès du Client et/ou auprès de sources externes.

Par ailleurs, le Client s'engage à fournir, à première demande, à la Banque, toute information et justificatif nécessaire, en cas d'opération(s) qui apparaîtrait(ont) à la Banque comme particulièrement complexe(s) ou d'un montant inhabituellement élevé ou dépourvue(s) de justification économique ou d'objet licite. A défaut de les fournir ou en cas de fourniture d'informations erronées par le Client, celui-ci est informé que la Banque se réserve la possibilité de ne pas exécuter l'opération ou de mettre un terme à l'opération et qu'elle pourra être conduite, en vertu des dispositions légales et réglementaires précitées, à résilier les conventions conclues avec le Client.

Le Client est informé que la Banque est tenue de déclarer les sommes inscrites dans ses livres et les opérations portant sur des sommes qui pourraient provenir d'une infraction passible d'une peine privative de liberté supérieure à un (1) an, ou qui pourraient être liées au financement du terrorisme. Ces obligations portent également sur les tentatives d'opérations. Ladite déclaration à la Cellule de Renseignement Financier est réalisée en application des dispositions des articles L. 561-15 et L. 561-18 du Code Monétaire et Financier.

Le Client est informé que les pouvoirs publics peuvent exiger de la Banque qu'elle n'exécute pas une opération demandée ou initiée par le Client, en application des dispositions de l'article L. 561-24 du Code Monétaire et Financier.

Pour la mise en œuvre de ces obligations et pendant toute la durée du Contrat, le Client s'engage envers la Banque :
- à respecter l'ensemble des obligations légales et règlementaires nationales relatives à la lutte contre le blanchiment d'argent et le financement du terrorisme ainsi que les législations étrangères équivalentes, dans la mesure où celles-ci sont applicables ;
- à ne pas utiliser, prêter, investir ou apporter ses fonds dans des opérations qui contreviendraient aux obligations de lutte contre le blanchiment de capitaux et le financement du terrorisme précitées ;

- à la tenir informée, sans délai, de toute modification survenue au niveau de ses situations personnelle, professionnelle, patrimoniale, financière ou de celles de sa caution éventuelle, et plus généralement de tout événement susceptible de modifier notoirement la valeur de son patrimoine ou d'aggraver l'importance de son endettement, ainsi que de toute modification relative à ses représentants légaux, actionnaires ou bénéficiaires effectifs ;
- à lui communiquer, à sa demande et sans délai, toute information, toute pièce ou tout document relatif à sa situation personnelle, professionnelle, patrimoniale ou financière ou aux conditions d'une opération inhabituelle initiée à son profit ou au profit d'un tiers.

Le Client est informé que la Banque est tenue de conserver, pendant cinq (5) ans à compter de la résiliation des conventions conclues avec le Client, l'ensemble des informations et documents le concernant, sans préjudice de l'obligation de conservation d'informations et documents le concernant pour d'autres produits et services fournis par la Banque, en application des dispositions de l'article L. 561-12 du Code Monétaire et Financier.

17.2 - Respect des sanctions internationales

La Banque est tenue de respecter les lois et réglementations en vigueur dans diverses juridictions, en matière de sanctions économiques, financières ou commerciales, et de respecter toute mesure restrictive liée à un embargo, à un gel des avoirs et des ressources économiques, à des restrictions sur des transactions avec des individus ou entités ou concernant des biens ou des territoires déterminés émises, administrées ou mises en place par le Conseil de sécurité de l'ONU, l'Union européenne, la France, les États-Unis d'Amérique (et notamment le Bureau de Contrôle des Actifs Etrangers rattaché au Département du Trésor : OFAC et le Département d'État) et par des autorités locales compétentes pour édicter de telles sanctions (ci-après les « Sanctions Internationales »).

Dans le cas où le Client, son mandataire éventuel, le bénéficiaire effectif, une contrepartie du Client, ou l'Etat dans lequel ils résident viendraient à faire l'objet de telles sanctions ou mesures restrictives, le compte du Client serait utilisé en violation des Sanctions Internationales, notamment pour recevoir ou transférer, de façon directe ou indirecte, des fonds en provenance ou à destination d'une contrepartie soumise directement ou indirectement aux Sanctions Internationales ou localisée dans un pays sous sanctions, la Banque pourra être amenée, en conformité avec celles-ci, à suspendre ou rejeter une opération de paiement ou de transfert émise et/ou reçue par le Client, qui pourrait être ou qui, selon son analyse, serait susceptible d'être sanctionnée par toute autorité compétente, ou le cas échéant, à bloquer les fonds et les comptes du Client ou à résilier le Contrat.

A ce titre, le Client déclare :
- Qu'il n'est pas une personne qui fait l'objet ou est la cible de Sanctions Internationales, ci-après une « Personne Sanctionnée » ;
- Qu'il n'est pas une personne située, constituée ou résident d'un pays ou un territoire qui fait, ou dont le gouvernement fait, l'objet d'un régime de Sanctions Internationales interdisant ou restreignant les relations avec ledit gouvernement, pays ou territoire ci-après un « Pays Sanctionné » ;
- Qu'il n'est pas une personne engagée dans une activité avec une Personne Sanctionnée ;
- Qu'il n'est pas une personne ayant reçu des fonds ou tout autre actif ou envoyé des fonds en provenance ou à destination d'une Personne Sanctionnée ;
- Qu'il n'est pas une personne engagée dans une activité avec une personne située, constituée ou résident d'un Pays Sanctionné.

Le Client s'engage envers la Banque, pendant toute la durée du Contrat :
- à informer sans délai la Banque de tout fait dont il aura connaissance qui viendrait rendre inexacte l'une ou l'autre des déclarations relatives aux Sanctions Internationales ;
- à ne pas utiliser directement ou indirectement ses fonds et à ne pas prêter, apporter ou rendre autrement disponible ses fonds à toute autre personne pour toute opération qui aurait pour objet ou effet le financement ou la facilitation des activités et des relations d'affaires avec une Personne Sanctionnée ou située, constituée ou résidente dans un Pays Sanctionné ou susceptibles de constituer une violation des Sanctions Internationales ;
- à n'utiliser aucun revenu, fonds ou profit provenant de toute activité ou pération réalisée avec une Personne Sanctionnée ou avec toute personne située, constituée ou résident d'un Pays Sanctionné dans le but de rembourser ou payer les sommes dues à la Banque au titre du présent contrat ;
- à la tenir informée sans délai de toute modification survenue au niveau de ses situations professionnelle, patrimoniale, financière ou personnelle ou de celles de sa caution éventuelle, et plus généralement de tout événement susceptible de modifier notoirement la valeur de son patrimoine ou d'aggraver l'importance de son endettement.

A défaut, la Banque se réserve la possibilité de ne pas exécuter l'opération ou de mettre un terme à l'opération.

ARTICLE 18 - LUTTE CONTRE LA CORRUPTION ET LE TRAFIC D'INFLUENCE

La Banque est tenue, dans le cadre de ses obligations légales et règlementaires (en particulier issues de la loi n° 2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique) concernant la lutte contre les atteintes à la probité, dont la corruption et le trafic d'influence, de procéder à l'évaluation de l'intégrité de sa clientèle pendant toute la durée de la relation d'affaires, au regard de critères de risques tels que :
- les bénéficiaires effectifs ;
- les pays de résidence et d'activité ;

- les secteurs d'activité ;
- la réputation et ;
- la nature, et l'objet de la relation ;
- les autres intervenants (écosystème) ;
- les interactions avec des agents publics ou des Personnes Politiquement Exposées (P.P.E) définies aux articles L. 561-10 1° et R. 561-18 du Code Monétaire et Financier et par les dispositions de l'arrêté ministériel du 17 mars 2023 fixant en application dudit article R. 561-18, la liste des fonctions françaises concernées ;
- les aspects financiers en jeu et devises traitées.

Le Client s'engage en conséquence :
- à permettre à la Banque de satisfaire aux obligations légales mentionnées ci-dessus visées, notamment en lui apportant toutes les informations nécessaires, spontanément ou à la demande de la Banque ;
- à ne pas effectuer sur ses comptes ouverts dans les livres de la Banque, d'opération(s) visant ou liée(s) à la commission d'un fait de corruption ou de trafic d'influence, de concussion, de prise illégale d'intérêt, de détournement de fonds publics ou de favoritisme, et à justifier sur demande les opérations sans objet apparent ;
- à ne pas proposer ou offrir de cadeaux, invitations ou autres avantages à un salarié de la Banque afin d'obtenir un avantage indu relatif au fonctionnement de ses comptes ouverts dans les livres de la Banque.

ARTICLE 19 - PROTECTION DES DONNÉES PERSONNELLES

Dans le cadre de la signature et de l'exécution du Contrat, la Banque recueille et traite des données à caractère personnel concernant les personnes physiques intervenant dans le cadre de ce Contrat (mandataire, représentant légal, caution, contact désigné, préposé, bénéficiaire effectif...).

Les informations expliquant pourquoi et comment ces données sont utilisées, combien de temps elles seront conservées ainsi que les droits dont ces personnes disposent sur leurs données figurent dans la Notice d'information de la Banque sur le traitement des données à caractère personnel. Cette notice est disponible à tout moment sur le site internet de la Banque via l'adresse suivante : https://www.caisse-epargne.fr/ile-de-france/protection-donnees-personnelles ou sur simple demande auprès de l'agence du Client. La Banque communiquera en temps utile les évolutions apportées à ces informations.

ARTICLE 20 - DURÉE ET RÉSILIATION

20.1 - Durée du contrat

Le Contrat prend effet à compter du jour de sa signature. Il est conclu pour une durée indéterminée.

20.2 - Résiliation sans motif

Chacune des parties peut mettre fin au présent contrat, par écrit (auprès de son agence ou par lettre recommandée avec demande d'avis de réception), à tout moment, sans avoir à indiquer ni justifier du motif.

Lorsqu'elle est effectuée par le Client, la résiliation devient effective au terme d'un délai de trente (30) jours à compter de la réception par la Banque de l'écrit adressé par le Client.

La résiliation par la Banque doit respecter un préavis de trente (30) jours.

Sauf indication contraire du Client, la résiliation de l'une des prestations optionnelles de CE net n'entraîne la résiliation que de cette seule prestation, l'abonnement de CE net continuant de produire ses effets entre les parties.

20.3 - Résiliation pour manquement

En cas de manquement par l'une quelconque des parties aux obligations dont elle a la charge au titre du Contrat, et auquel il n'aurait pas été remédié dans un délai de huit (8) jours à compter de l'envoi d'une lettre recommandée avec demande d'avis de réception, l'autre partie pourra, prononcer la résiliation de la Convention.

20.4 - Résiliation de plein droit

La résiliation de la convention de compte courant entraîne la résiliation automatique du Contrat.

20.5 - Effets de la résiliation

En cas de cessation de la Convention, pour quelque motif que ce soit, les Parties sont tenues de prendre toutes dispositions utiles en vue du dénouement des opérations en cours. Tout ordre donné avant la date effective de résiliation est exécuté aux conditions et dates convenues. Le Client n'aura plus accès à l'ensemble des fonctionnalités et services disponibles depuis CE net.

La résiliation du Contrat entraîne de plein droit la résiliation du service de Signature électronique et/ou d'Authentification forte sur CE net liés au Contrat.

20.6 - Possibilité de suspension par la Banque

La Banque se réserve le droit de bloquer sans délai, sans aucun préavis, ni formalité, le service CE net, ou une Personne habilitée, pour des raisons objectivement motivées liées à la sécurité du Service, à la présomption d'une utilisation non autorisée ou frauduleuse du Service ou au risque sensiblement accru ou avéré que le Client soit dans l'incapacité de s'acquitter de son obligation de paiement. Dans ces cas, la Banque informe le Client, par tous moyens, du blocage et des raisons de ce blocage, si possible avant que le Service ne soit bloqué ou immédiatement après sauf si cette information est impossible pour des raisons de sécurité ou interdite par une législation communautaire ou nationale. La Banque débloque le Service dès lors que les raisons du blocage n'existent plus.

ARTICLE 21 - RÉCLAMATIONS - MÉDIATION

En cas de difficultés concernant ces produits et services, le Client peut obtenir de son Agence toutes les informations souhaitées, formuler auprès d'elle toute réclamation et/ou saisir par écrit le « Service Relations Clientèle » de la Banque qui s'efforce de trouver avec lui une solution, y compris si la réponse ou solution qui lui a été apportée par son Agence ne lui convient pas.

Le Client trouvera les coordonnées du service en charge des réclamations dans les brochures tarifaires de la Banque ainsi que sur son site internet, dans la rubrique « Contact » ou en saisissant « Réclamation » dans le moteur de recherche.

La Banque s'engage à accuser réception de la réclamation du Client sous dix (10) Jours Ouvrables à compter de sa date d'envoi, sauf si une réponse peut être apportée dans ce délai. Si une analyse plus approfondie de son dossier est nécessaire, la Banque s'engage à lui apporter une réponse dans un délai qui ne pourra excéder deux (2) mois (à compter de la date d'envoi de sa réclamation).

Concernant les réclamations liées aux services de paiement, une réponse sera apportée au Client dans les quinze (15) Jours Ouvrables suivant la réception de sa réclamation. Cependant, si un délai supplémentaire est nécessaire pour lui répondre, la Banque lui adressera une réponse d'attente motivant ce délai et précisant la date ultime de sa réponse. En tout état de cause, le Client recevra une réponse définitive au plus tard trente-cinq (35) Jours Ouvrables suivant la réception de sa réclamation.

A défaut de solution le satisfaisant ou en l'absence de réponse dans ces délais, le Client, dès lors qu'il est un Entrepreneur individuel au sens de l'article L. 526-22 du Code de Commerce et uniquement dans ce cas, a la faculté de saisir gratuitement le médiateur de la Banque sur son site internet ou par voie postale, dans le délai d'un (1) an à compter de sa réclamation auprès de la Banque, sans préjudice des autres voies d'actions légales dont il dispose.

L'adresse postale du médiateur et les coordonnées du site internet du médiateur figurent sur les brochures tarifaires et le site internet de la Banque.

Les informations nécessaires à la saisine du médiateur, son périmètre et le déroulé de la procédure de médiation figurent sur la charte de médiation disponible sur le site internet du médiateur.

ARTICLE 22 - LANGUE ET DROIT APPLICABLES - ATTRIBUTION DE COMPÉTENCE

Le Contrat est conclu en langue française. Le Client accepte expressément l'usage de la langue française durant les relations contractuelles et précontractuelles.

Le Contrat est soumis au droit français.

En cas de contestation, pour quelque cause que ce soit, la Banque et le Client porteront tout litige auprès du Tribunal compétent dans le ressort duquel est situé le siège social de la Banque. Cette stipulation n'est applicable que si le Client a la qualité de commerçant.

ARTICLE 23 - ÉLECTION DE DOMICILE

Pour l'exécution du Contrat, il est fait élection de domicile par la Banque, en son siège social ou au lieu de son établissement principal, par le Client, au lieu d'exercice de son activité, à son adresse ou à son siège social indiqué aux Conditions Particulières.

ARTICLE 24 - DOCUMENTS CONTRACTUELS

Les documents contractuels applicables par ordre de préséance sont :

- De manière égale, les Conditions Particulières, comprenant en annexe les synthèses des habilitations, la synthèse des délégations des signatures et la synthèse du Collège de signature,
- Les présentes Conditions Générales,
- La Convention de compte courant,
- Les contrats liés aux différents protocoles utilisés (EBICS, SWIFTNET),
- Les autres contrats négociés par ailleurs entre les Parties.