CONDITIONS GENERALES DU SERVICE CREDIT COOPERATIF DIRECT
En vigueur à compter du 9 octobre 2025

Préambule

Le présent contrat relatif au service de banque à distance Crédit Coopératif Direct se compose des présentes conditions générales, des conditions particulières et des conditions tarifaires applicables, ainsi que de ses éventuels annexes et avenants.

Le présent contrat est complété :

- par la convention de compte de dépôt,

- par toutes autres conventions existantes liées à des services spécifiques signées par le Client, par acte séparé.

Les opérations acceptées dans le cadre du présent service de banque à distance ne sauraient déroger aux conditions particulières et/ou générales d'autres produits ou services ouverts ou à ouvrir, sauf stipulation contraire.

En cas de contradiction entre les présentes conditions générales et les conditions particulières, les dispositions contenues dans ces dernières priment.

1 - Objet

L'abonnement au service de banque à distance Crédit Coopératif Direct (ci-après dénommé le « Service ») permet au Client (ci-après « le Client ») d'accéder à un ensemble de services rendus par le Crédit Coopératif (ci-après dénommé la « Banque »), utilisant les nouvelles technologies (internet, téléphone fixe, mobile …), pour consulter et/ou réaliser à distance, tout ou partie, des opérations sur le ou les compte(s) et produits ouverts dans les livres de la Banque ou souscrit(s) par son intermédiaire.

Sont concernés les comptes ouverts et/ou les contrats souscrits par le Client à la date d'adhésion au Service et ceux ouverts et/ou souscrits ultérieurement.

La détention d'un compte de dépôt ou d'un compte d'épargne par le Client n'est pas obligatoire pour avoir accès au Service. Les modalités de fonctionnement du Service sont dans ce cas adaptées aux produits ou services détenus ou à souscrire, ou sur lesquels le Client intervient en qualité de mandataire.

Certaines des opérations ci-dessous décrites peuvent, en fonction du canal ou du type de terminal utilisé, ne pas être accessibles au moment de l'adhésion au Service. Les nouvelles fonctionnalités seront progressivement mises à disposition par la Banque. Le Client en sera informé par tout moyen.

La Banque se réserve le droit de modifier le contenu du Service en vue d'en améliorer la qualité, notamment, par l'adjonction de nouvelles fonctionnalités. Dans ce cas, le Client sera informé des impacts contractuels et tarifaires éventuels, dans les conditions prévues à l'article 9.1 ci-dessous.

Le Service est disponible sur l'espace de banque à distance du Client 24 heures sur 24 et 7 jours sur 7 accessible soit, via le site internet de la Banque, soit, via l'application mobile de la Banque à télécharger préalablement (ci-après « **Espace personnel de banque à distance** »).

référence interne n° CG4BA01CCD scellé électroniquement le 16/07/2025

2 - Clientèle concernée

a- Dispositions générales

Le Service est accessible aux personnes physiques :

- majeures capables,
- majeures protégées. Pour les personnes sous sauvegarde de justice avec mandataire spécial, en curatelle simple, en curatelle renforcée, en tutelle, avec habilitation familiale spéciale ne statuant pas sur la gestion des comptes bancaires, avec mandat de protection future activé, faisant l'objet d'une Mesure d'Accompagnement Social Personnalisée Renforcée ou d'une Mesure d'Accompagnement Judiciaire, le Service est ouvert avec l'accord du curateur, du tuteur, de la personne habilitée, du représentant légal ou du mandataire.
- Mineures avec l'autorisation du représentant légal, dans les conditions définies ci-après.

Le Service est utilisé par le Client à des fins personnelles et non pour des besoins professionnels.

Le cas échéant, le Client peut conférer à un tiers une procuration spécifique sur un ou plusieurs de ses comptes et/ou contrats, ce tiers devant lui-même adhérer au Service afin de disposer de ses propres identifiant, mot de passe et code d'authentification.

En cas de compte joint, l'un et/ou l'autre titulaire peut(vent) être abonné(s) au Service. Chaque co-titulaire disposera de son propre identifiant, mot de passe et code d'authentification.

b- Curatelle renforcée, tutelle, habilitation familiale, mandat de protection future et mesures d'accompagnement

Pour les majeurs en curatelle renforcée, en tutelle ou avec habilitation familiale, avec mandat de protection future activé, faisant l'objet d'une Mesure d'Accompagnement Social Personnalisée Renforcée ou d'une Mesure d'Accompagnement Judiciaire, les fonctionnalités du Service seront limitées à la consultation des comptes de dépôt dont ils sont titulaires. Les comptes d'épargne ne peuvent être consultés qu'avec l'accord préalable du représentant légal.

Les autres fonctionnalités seront utilisées par le représentant légal (curateur, tuteur, personne habilitée, mandataire…), à partir de son Espace personnel de banque à distance pour consulter et gérer le(les) compte(s) du Client.

c- Enfant mineur

Par dérogation à l'article 1, l'Espace personnel de banque à distance du mineur est accessible uniquement via l'application mobile de la Banque. L'accès aux fonctionnalités du Service est adapté en fonction de l'âge du mineur.

Jusqu'à 16 ans, l'accès au Service par le mineur est limité uniquement à la consultation de son compte, à certaines fonctionnalités de gestion en ligne de sa carte bancaire, à la réception des alertes liées à ses comptes ou sa carte bancaire et à la réalisation de virements internes entre son compte de dépôt et un autre de ses comptes de dépôt ou comptes/produits d'épargne ouverts dans les livres de la Banque et sous réserve, le cas échéant, que son représentant légal ait autorisé que ces comptes et produits d'épargne soient affichés dans son Espace personnel de banque à distance.

A partir de 16 ans, le mineur pourra avoir accès à la fonctionnalité de virements externes et au service Wero avec l'autorisation préalable de l'un de ses représentants légaux client de la Banque, selon les modalités décrites à l'article 3.

Les représentants légaux sont admis à effectuer des opérations pour le compte de leurs enfants mineurs. Chaque représentant légal reconnaît que l'opération réalisée par un des représentants légaux du mineur est réputée avoir reçu l'accord de l'autre.

Dans l'hypothèse où un représentant légal s'opposerait à ce mode de fonctionnement, il devrait adresser un courrier recommandé avec avis de réception ou remis en main propre contre décharge ou un message MSI à l'agence gestionnaire du compte. Le Service sera alors résilié par la Banque.

3 – Description détaillée du Service

a- Consultation des comptes et produits et réalisation des opérations

Sous les conditions définies par la Banque, le Service permet au Client de :

- Consulter ses comptes de dépôt, comptes d'épargne et comptes d'instruments financiers ouverts dans les livres de la Banque et ses crédits et assurances souscrits auprès de la Banque,
- Réaliser des opérations sur ces comptes et produits,
- Visualiser l'historique des opérations de ces comptes et produits et piloter sa(ses) carte(s) bancaire(s) dans son Espace personnel de banque à distance.

L'utilisation du Service peut être limitée uniquement à la consultation des comptes.

b- Virements

Le Client peut effectuer des virements :

- de l'un de ses comptes de dépôt vers un autre de ses comptes de dépôt ou vers un compte de dépôt de tiers ouvert à la Banque ou dans les livres de tout autre établissement de crédit.
- de sa réserve de crédit renouvelable vers l'un de ses comptes de dépôt ouvert à la Banque.
- de l'un de ses comptes de dépôt vers un compte d'épargne ouverts à la Banque ou à partir d'un compte d'épargne vers l'un de ses comptes de dépôt ouvert à la Banque.

Les caractéristiques des services de virements et les modalités d'exécution des virements sont décrites dans la convention de compte de dépôt et, le cas échéant, de compte d'épargne, en vigueur.

Avant l'âge de 16 ans, le mineur peut réaliser uniquement des virements internes entre son/ses compte(s) de dépôt et son/ses compte(s)/produit(s) d'épargne, et inversement, ouverts dans les livres de la Banque, selon les règles de gestion définies dans les conventions de comptes/produits d'épargne concernées et sous réserve, le cas échéant, que son représentant légal ait autorisé que ces comptes et produits d'épargne soient affichés dans son Espace personnel de banque à distance.

Le mineur, à partir de 16 ans, peut être autorisé par l'un de ses représentants légaux, à effectuer seul des virements externes (virements SEPA classiques, virements SEPA instantanés et virements instantanés via Wero). Concernant les virements SEPA classiques et virements SEPA instantanés, le client mineur pourra ajouter au préalable des bénéficiaires, dans son Espace personnel de banque à distance. Grâce à cette autorisation, il pourra aussi activer et utiliser seul le service Wero. L'autorisation du représentant légal est consentie via la rubrique spécifique « contrôle parental » disponible dans la rubrique Réglages de l'application mobile de la Banque, en utilisant le dispositif d'authentification forte Sécur'Pass, ou en agence auprès de la Banque (sous réserve de disponibilité).Cette autorisation peut être retirée, à tout moment, par le représentant

légal, via cette rubrique, ce qui entraîne automatiquement la désactivation de la fonctionnalité de virements externes et du service Wero. Le mineur et son autre représentant légal, client de la Banque, seront informés de cette autorisation ou du retrait de celle-ci par une notification adressée par la Banque.

A sa majorité, le mineur recouvre la faculté de réaliser seul des virements externes sans l'autorisation préalable de l'un de ses représentants légaux.

L'émission de virements vers un tiers nécessite que le Client ajoute préalablement le compte du bénéficiaire sur sa liste de bénéficiaires de virements. L'ajout de ce compte sur cette liste de bénéficiaires ainsi que l'émission d'un virement externe nécessitera l'authentification du client.

En revanche, l'émission d'un virement vers un compte dont le Client est titulaire, ouvert dans les livres de la Banque, ne donnera pas lieu à cette authentification.

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.

- **Limites de montant maximal (plafond) pour l'émission des virements SEPA classiques et instantanés**

Il est convenu entre le Client et la Banque que les virements SEPA classiques et instantanés externes, réalisés par le Client via son Espace personnel de banque à distance, sont limités par les plafonds cumulatifs suivants : un plafond par opération, un plafond journalier et un plafond mensuel.

Ces plafonds peuvent être consultés par le Client dans la rubrique « Plafonds de virements » de son Espace personnel de banque à distance accessible via l'application mobile de la Banque.

Le Client majeur, habilité à réaliser des virements, a la possibilité de modifier, à tout moment, à la hausse ou à la baisse, chacun des plafonds, dans cette rubrique de son Espace personnel de banque à distance, accessible via l'application mobile de la Banque. Le Client doit confirmer le nouveau plafond en utilisant le dispositif d'authentification forte Secur'Pass. En cas d'augmentation du plafond par opération ou du plafond journalier, les autres plafonds sont automatiquement ajustés. En revanche, en cas d'augmentation du plafond mensuel, les autres plafonds restent inchangés.

Si le nouveau plafond choisi par le Client excède le plafond défini par la Banque, le Client doit envoyer une demande d'augmentation du plafond auprès de son conseiller en agence via son Espace personnel de banque à distance, en utilisant le dispositif d'authentification forte Secur'Pass. Le Client peut suivre l'avancement de sa demande dans la rubrique « Plafonds de virements ». Il ne peut soumettre aucune autre demande d'augmentation de plafond tant que sa demande est en cours de traitement par le conseiller. Si sa demande est acceptée, le Client en reçoit la confirmation par e-mail et par notification. Le nouveau plafond est temporaire et

valable jusqu'à la date indiquée dans son Espace personnel de banque à distance. En cas de refus de sa demande de dépassement de plafond, le Client en est également informé par e-mail et par notification.

Lorsque le montant du virement initié par le Client excède l'un des plafonds applicables, la Banque l'informe que le virement ne peut pas être exécuté et lui indique qu'il peut modifier le plafond concerné dans son Espace personnel de banque à distance accessible via son application mobile.

Pour un client mineur, la demande de modification de plafond doit être effectuée auprès du conseiller en agence, par l'un des représentants légaux ou en cas de dépassement du plafond défini par la Banque, par les deux représentants légaux.

La Banque est également susceptible d'appliquer des mesures complémentaires visant à protéger le Client de tout risque d'utilisation frauduleuse de son abonnement. De même, en cas de suspicion de fraude ou de fraude avérée, la Banque aura la faculté d'abaisser automatiquement et temporairement les plafonds appliqués aux virements effectués par le Client dans son Espace personnel de banque à distance. Le Client sera ensuite informé par la Banque, par tout moyen et dans les meilleurs délais, des modalités de rétablissement des plafonds initialement prévus.

- **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 personnel 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 du contrôle**

Cette vérification est effectuée sur la base des informations fournies par le prestataire de services de paiement du bénéficiaire.

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

Dans les autres cas, la Banque informe immédiatement le Client, dans le parcours du virement, du résultat de la vérification réalisée.

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 sans corriger le nom du bénéficiaire, 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. Lorsqu'ils ne concordent pas, la Banque doit en informer la banque du payeur. 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.

c - Contrôle parental (sous réserve de disponibilité)

Le Client, représentant légal d'un mineur client de la Banque, peut fixer des conditions et limites à l'utilisation du compte de son enfant mineur ou des services associés à ce compte, par l'intermédiaire de la rubrique « Contrôle parental » disponible dans la rubrique Réglages de l'application mobile de la Banque. Ces limites s'appliqueront automatiquement dans l'espace de banque à distance du mineur. Il peut ainsi :

- autoriser le mineur, à partir de 16 ans, à effectuer des virements externes et ainsi à activer et à utiliser seul le service Wero ou retirer cette autorisation. Le mineur doit avoir préalablement téléchargé l'application mobile de la Banque et activé Sécur'Pass ;
- choisir que les comptes, produits d'épargne et contrats d'assurance de l'enfant mineur soient affichés ou non dans l'espace personnel de banque à distance de ce dernier.

Par ailleurs, dans le menu cartes de son espace de banque à distance, le client représentant légal peut gérer la carte bancaire de son enfant mineur (Cf. ci-après, paragraphe n - Fonctionnalités de pilotage de la carte).

d – Réception de virements via Wero – Client adhérent ou non à ce service

Le service Wero, produit d'EPI Company, est accessible gratuitement à partir de l'application bancaire mobile de la Banque.

Le service Wero permet, via l'application bancaire mobile de la Banque et sous réserve d'avoir accepté les Conditions Générales d'Utilisation spécifiques, d'émettre un virement SEPA instantané de particulier à particulier, en saisissant le numéro de téléphone mobile du bénéficiaire, sans avoir à compléter les coordonnées bancaires du compte (IBAN) de ce dernier.

Afin de faciliter la réception de virements via Wero, pour un client personne physique majeure capable ou mineure, à partir de 16 ans, autorisée à effectuer des virements externes par l'un de ses représentants légaux, titulaire d'un abonnement de banque à distance, la Banque peut communiquer à EPI Company, son numéro de téléphone mobile personnel déclaré auprès de son agence. L'IBAN de son compte de dépôt ouvert dans les livres de la Banque ne sera communiqué qu'à condition que ce numéro de téléphone mobile personnel ne soit pas déjà associé à un autre IBAN dans la base de données décrite ci-dessous.

Ces données personnelles sont communiquées à EPI Company afin d'alimenter la base de données centralisée et sécurisée administrée par ce prestataire de la Banque en vue du fonctionnement de ce service. Cette base de données réalise la correspondance entre les numéros de téléphone mobile et les IBAN des bénéficiaires des virements effectués via le service Wero.

Ces traitements de données personnelles sont réalisés sur la base de l'intérêt légitime de la Banque à faciliter l'utilisation du service Wero par ces clients et pour cette seule finalité.

S'il y a lieu, le Client est informé de la communication de ses données personnelles à EPI Company par courrier électronique. Cette information rappellera les données communiquées afin de recevoir automatiquement des virements via Wero. Elle rappellera également comment s'opposer à ce traitement.

Le Client, bénéficiaire d'un virement via Wero, sera également informé, par une notification hors Application mobile de la Banque, du montant du virement, du nom de l'émetteur et du compte crédité. Le nom de l'émetteur sera anonymisé dans le cadre du service Wero.

Le Client a la possibilité de s'opposer, gratuitement et à tout moment, à ce que ses données soient traitées par la Banque et par EPI Company, selon les modalités prévues dans la Notice d'information sur le traitement des données à caractère personnel.

Il est précisé que les données du Client seront supprimées de la base de données gérée par EPI Company en cas de :

- Demande de suppression/opposition formulée par le Client ;
- Clôture du compte de dépôt ouvert dans les livres de la Banque ;
- Résiliation du contrat de banque à distance ou blocage de l'accès au service de banque à distance ;
- Absence de numéro de téléphone mobile déclaré ou de validation de ce numéro par le client.

Il est également précisé que le Client, bénéficiant de la communication de ses données vers EPI Company, doit activer le service pour émettre un virement via le service Wero.

e- Consultation de l'historique des prélèvements exécutés, à venir et rejetés et blocage/réactivation des prélèvements

Le Client peut consulter dans son Espace personnel de banque à distance la liste des prélèvements exécutés, à venir et rejetés.

Les fonctionnalités de blocage ou de réactivation des prélèvements sont également disponibles dans l'Espace personnel de banque à distance du Client.

f- Opérations sur instruments financiers et autres titres.

Pour pouvoir effectuer les opérations sur instruments financiers, le Client doit avoir au préalable signé une convention de compte d'instruments financiers auprès de la Banque.

Dans le respect des conditions de fonctionnement de cette convention, des règles de couverture et des conditions de passation des ordres, le Client peut passer tous ordres conformément aux règles et pratiques des marchés y compris tous ordres sur les OPC (Organismes de Placement Collectif) du Réseau Crédit Coopératif.

Les comptes d'instruments financiers indivis et ceux ouverts en nue-propriété avec réserve d'usufruit ne peuvent pas faire l'objet d'opérations dans le cadre du Service.

La souscription définitive des ordres d'achat de titres de sociétés en cours de privatisation et la souscription de titres d'emprunts sont subordonnées à la réception par la Banque, dans les délais imposés par la réglementation, des documents afférents à ces opérations dûment signés.

Les ordres ne pourront être acheminés sur le marché qu'aux jours et heures d'ouverture des Marchés financiers.

Conformément aux dispositions de la convention de compte d'instruments financiers, le Client sera informé par voie d'avis d'opéré de l'exécution de ses ordres sur instruments financiers dès leur réalisation. Le Client s'oblige donc à exercer ce contrôle dès sa réception et le cas échéant, à saisir immédiatement la Banque de toute anomalie ou cause de contestation. Les informations figurant sur l'avis d'opéré, non contestées dans les deux jours calendaires de leur réception, seront considérées comme approuvées. En tout état de cause, toute réclamation sera prescrite dans les 6 (six) mois de la conclusion de l'opération contestée. Les contestations doivent être formulées par écrit et être motivées.

Si le Client souscrit au service « e-Documents », les avis d'opérés seront mis à disposition sur son Espace personnel de banque à distance. Le Client sera informé de cette mise à disposition dans sa Messagerie Sécurisée Internet et par courriel dans sa messagerie personnelle à l'adresse e-mail indiquée lors de la souscription du service e-Documents.

g – Opérations sur les contrats d'assurance

Le Client peut également effectuer, par l'intermédiaire du Service, des actes de gestion sur ses produits d'assurance.

Les partenaires assureurs acceptent, pour les opérations relatives à ces produits accessibles par le Service, l'ensemble des dispositions figurant aux articles 5, 6 et 7 ci-dessous, en ce qui concerne les modalités de preuve. Le Client est tenu, à leur égard, aux mêmes dispositions que celles figurant auxdits articles.

h – Rubrique « Souscrire »

Le Client peut souscrire, dans le respect de la réglementation en vigueur applicable, à certains services offerts par la Banque. La souscription effective du service ou la prise en compte d'un avenant peut être subordonnée au renvoi du contrat ou de l'avenant signé dans les délais qui seront indiqués au Client. Le cas échéant et sous réserve de disponibilité du service, le Client peut également procéder à la signature électronique de certains contrats via son espace personnel de banque à distance, notamment, un crédit ou une opération en lien avec ses crédits.

Dans le cadre de son abonnement au Service, le Client peut accéder à certains services proposés par la Banque ou ses partenaires, exclusivement par le Service. L'accès effectif s'effectue après activation du service par ses soins et acceptation de Conditions Générales d'Utilisation spécifiques, distinctes du présent contrat. Le Client peut également désactiver certains services par l'intermédiaire du Service. Cette désactivation vaut résiliation du contrat et du service concerné.

i - Commande de chéquiers (sous réserve de disponibilité)

Le Client peut commander ses chéquiers sur son Espace personnel de banque à distance. Le nombre total de chéquiers commandés quel que soit le canal (agence, GAB, Espace personnel de banque à distance) ne peut excéder le nombre maximal en commande par Client, fixé par la Banque. Le Client est invité à se renseigner en agence. L'enregistrement de la commande s'effectue à l'expiration d'un délai de 48 heures ouvrées.

j - Messagerie Sécurisée Internet

Dans le cadre de son abonnement au Service et après une connexion à son Espace personnel de banque à distance, le Client a accès à une messagerie électronique dans l'environnement sécurisé du Service, la « Messagerie Sécurisée Internet » (ci-après « MSI »), dont les Conditions Générales d'Utilisation figurent à l'article 11 ci-après. Le Client est informé que le premier accès à la MSI vaut acceptation de ces CGU dont il doit prendre connaissance au préalable. Les messages sont consultables par le Client pendant un délai de 90 jours à compter de leur réception.

k – Service d'agrégation de comptes

Dans le cadre de son abonnement au Service, le Client peut avoir accès à un service d'agrégation de comptes gratuit permettant notamment d'accéder à des fonctionnalités d'agrégation de comptes étendues. Ces fonctionnalités nécessitent l'acceptation préalable de Conditions Générales d'Utilisation distinctes.

La résiliation de l'abonnement au Service entraîne la fermeture du service d'agrégation de comptes.

l - Catégorisation de dépenses et de revenus

Cette fonctionnalité permet de catégoriser automatiquement les opérations du Client enregistrées sur son compte (individuel ou joint). Les écritures catégorisées sont disponibles pendant une période de 26 mois glissants à partir de la date de l'opération. Les opérations sont classées dans diverses catégories (Alimentation, Logement…), permettant de disposer d'une meilleure lisibilité des dépenses et revenus. Le Client a la possibilité de modifier la catégorisation d'une opération. En cas de résiliation de l'abonnement au Service, l'ensemble des personnalisations et des catégorisations seront alors définitivement perdues.

m - Localisation des commerçants auprès desquels le Client a effectué une opération de paiement :

Cette fonctionnalité permet au Client, qui consulte au moyen du Service le détail d'une opération de paiement qu'il a réalisé par carte bancaire, d'afficher sur un plan l'adresse du commerçant auprès duquel ladite opération a été effectuée. Cet affichage est réalisé sur la base des coordonnées GPS de l'adresse que le commerçant a préalablement déclarée, et est matérialisé par la visualisation d'un repère sur un plan généré par une application de cartographie (Google Maps, Plans) installée sur le matériel du Client et utilisant son adresse IP.
Dans ce cadre, le Client reconnaît avoir pris connaissance des conditions générales relatives à l'utilisation de l'application de cartographie qu'il utilise, disponibles auprès de Google ou Apple :

- Google Maps : https://policies.google.com/privacy
- Plans (Apple) : https://www.apple.com/legal/privacy/

Seules les opérations de paiement réalisées par carte bancaire chez des commerçants équipés de terminaux de paiement électroniques sont concernées par cette fonctionnalité, à l'exclusion des opérations réalisées à distance.
Le Client est informé que l'affichage de l'adresse du commerçant n'a qu'une valeur indicative, la Banque ne saurait être tenue pour responsable d'une erreur ou d'une absence de mise à jour de ses coordonnées GPS par le commerçant.
Par ailleurs, le Client peut à tout moment choisir de désactiver cette fonctionnalité dans les paramètres du Service.

n - Fonctionnalités de pilotage de la carte

Dans le cadre de son abonnement au Service, le Client, détenteur d'une carte bancaire émise par la Banque, peut avoir accès à des fonctionnalités de gestion en ligne de sa carte dans son Espace personnel de banque à distance sur le site internet de la Banque et/ou sur son application bancaire mobile. Ces fonctionnalités : paiements à distance, paiements et retraits à l'étranger, verrouillage temporaire, consultation des plafonds de paiement et de retrait, augmentation temporaire de ces plafonds, mise en opposition de la carte avec effet immédiat, consultation de son code secret, utilisation digitale de la carte, levée de doute sur des opérations inhabituelles, contestation d'opérations, etc ..., sont décrites dans les Conditions générales de son Contrat Carte.

L'activation ou la désactivation de l'une quelconque de ces fonctionnalités par le Titulaire de la Carte s'effectue sous sa responsabilité. Elle pourra nécessiter l'utilisation du dispositif d'authentification forte Sécur'Pass que le Titulaire de la Carte doit avoir préalablement activé dans son application bancaire mobile.
Cette activation ou désactivation est en principe opérationnelle en temps réel, sous réserve des délais techniques d'exécution ou de l'indisponibilité momentanée du service (exemple : maintenance).
Si la fonctionnalité est soumise à tarification, cette dernière est précisée dans les Conditions et Tarifs de la Banque applicables au Titulaire de la Carte.

Certaines fonctionnalités ne sont pas disponibles en tout ou en partie pour les titulaires de cartes mineurs ou majeurs protégés. En revanche, leur représentant légal peut, sous certaines conditions, gérer leur carte à distance via son propre Espace personnel de banque à distance, via la rubrique carte de tiers. Ces conditions et les fonctionnalités disponibles pour les titulaires de cartes mineurs ou majeurs protégés sont précisées sur le site internet de la Banque.

Depuis l'application mobile de la Banque, dans la rubrique lui permettant de gérer sa carte, le Client peut également enrôler sa carte dans la solution de paiement mobile Apple Pay sur le même iPhone où il a téléchargé cette application mobile. Lors de cet enrôlement, il devra s'authentifier par Sécur'Pass.

A partir de cette même rubrique, le Client peut souscrire au service e-cartes (sous réserve de disponibilité) pour sa carte VISA ou chacune de ses cartes VISA ou pour une carte VISA appartenant à un tiers. Ce service lui permet (ou permet au porteur de la carte, dans son propre Espace personnel de banque à distance) de créer une ou plusieurs e-cartes, afin de payer des achats sur internet, sans communiquer les données de sa carte.

o – Consultation des contrats signés électroniquement par le Client

Le Client peut consulter, télécharger et/ou imprimer ses contrats signés électroniquement avec la Banque dans son Espace personnel de banque à distance.

p – Mes Alertes

La fonctionnalité « Mes alertes » vise à mettre à disposition de chaque client, abonné au Service, un service d'alertes personnalisées en temps réel en rapport avec des événements ayant une incidence sur la gestion de son compte ou de sa carte bancaire. Les alertes sont activables sur l'ensemble des comptes de dépôt, comptes d'épargne (Livret A, Livret Jeune, LDDS, LEP, Compte sur Livret, PEL et CEL) et cartes pour lesquels le Client est titulaire, représentant légal ou mandataire.

4 - Exécution des opérations

Dès validation, notamment électronique, l'ordre est enregistré et est irrévocable. Les opérations sont exécutées sous réserve du solde du ou des comptes du Client et de ses autres engagements. Les opérations passées via le Service seront enregistrées par la Banque dans le cadre des usages bancaires et financiers d'imputation.

5 - Accès aux services

5.1 Les moyens matériels et techniques

Le Client accède au Service, par un matériel compatible (ordinateur multimédia, téléphone fixe, smartphone ou tablette et objets connectés à ces derniers).

Il appartient au Client de se procurer à ses frais et sous sa responsabilité les matériels et équipements appropriés ainsi que les moyens de communication (abonnements, accès à Internet…) nécessaires à l'utilisation par Internet du Service. Le Client devra également disposer d'un logiciel compatible dont les fonctions JavaScript et Cookies sont activées.

Pour l'Application mobile de la Banque, il est nécessaire d'avoir une version minimum du système d'exploitation de l'appareil utilisé, selon les précisions indiquées dans les espaces de téléchargement d'applications (Google Play, Apple Store, etc…).

La mise à jour du matériel, de l'équipement, du système d'information ou des applicatifs de ces matériels est sous la responsabilité du Client.

5.2 Modalités d'identification et d'authentification

5.2.1 Principes d'utilisation

Le Client dispose d'un identifiant qui lui est propre. Pour accéder au Service, le Client doit saisir cet identifiant et le mot de passe associé et utiliser un dispositif d'authentification forte, chaque fois que la Banque le lui demande.

Lors de l'ouverture du Service, l'identifiant ainsi qu'un mot de passe provisoire sont attribués au Client.

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 au Service, ou de supprimer certains dispositifs d'authentification moyennant une information du Client par tout moyen au choix de la Banque.

Les dispositifs d'identification et d'authentification forte mis à disposition par la Banque peuvent être utilisés pour, à partir de l'Espace personnel de banque à distance du Client, lui permettre d'accéder au site ou à l'application d'une entreprise du Groupe BPCE avec laquelle le Client entre ou est en relation, y être automatiquement identifié sans autre saisie d'un identifiant et d'un mot de passe, et y authentifier toute transaction portant sur les produits ou services à souscrire ou souscrits directement auprès de celle-ci.

5.2.2 Mot de passe

Lors de l'ouverture du contrat, l'identifiant ainsi qu'un mot de passe provisoire sont attribués au Client.

Le Client est tenu de modifier son mot de passe lors de sa première connexion.

Ce mot de passe pourra être modifié, à tout moment, par le Client et à sa seule initiative et par la Banque pour des mesures de sécurité. Toute modification de ce mot de passe est valable pour l'ensemble des canaux d'accès au Service : téléphone, internet, mobile.

Il est conseillé au Client de ne pas choisir un mot de passe aisément décelable par un tiers. Il ne doit jamais être indiqué sur les écrits ou messages électroniques adressés à la Banque, ou être mentionné sur les répondeurs téléphoniques.

Après plusieurs tentatives infructueuses de saisie du mot de passe, le dispositif d'accès au Service devient inopérant. Dans ce cas, le service sera de nouveau accessible sur demande du Client auprès de son agence.

5.2.3 Dispositif d'authentification forte

Le Client doit également être équipé de l'un des dispositifs d'authentification forte proposés par la Banque :

-Sécur'Pass : fonction d'authentification intégrée à l'application mobile de la Banque et couplée à un code confidentiel (détaillé à l'article 5.2.4) ;

-Code à usage unique mis à disposition par SMS, en complément du mot de passe saisi préalablement par le Client pour l'accès au Service. Le Client doit avoir préalablement communiqué son numéro de téléphone mobile à la Banque, dans les conditions communiquées par la Banque ;

- Lecteur d'authentification par carte à puce associé à une carte bancaire ou une carte d'authentification, permettant d'obtenir un code à usage unique ;

- autre dispositif éventuellement proposé par la Banque.

L'utilisation de ce dispositif d'authentification forte conduit à la saisie d'un code spécifique (ci-après « Code »), qui correspond au code Sécur'Pass, au code à usage unique transmis par SMS ou généré par le lecteur d'authentification par carte à puce.

La saisie de ce Code sera exigée par la Banque lors du premier accès au Service, puis à intervalle régulier ou chaque fois que cela s'avère nécessaire pour des raisons de sécurité, dans les conditions prévues par la législation.

Le Client peut paramétrer et utiliser la fonction biométrique de son smartphone, pour permettre une saisie automatique de ce Code.

L'utilisation de ce dispositif d'authentification forte pourra aussi être requise, dans les conditions prévues par la législation, pour la réalisation des opérations de paiement (virements), des opérations sensibles (ajout d'un compte de bénéficiaire de virement, enregistrement ou modification d'un ordre de virement permanent…) par l'intermédiaire du Service.

La Banque pourra appliquer des exceptions à la mise en place de ce dispositif d'authentification forte du Client dans les conditions et selon les limitations prévues par la réglementation en vigueur.

5.2.4 Sécur'Pass

Sécur'Pass est un dispositif d'authentification forte que le Client doit activer sur l'application mobile de la Banque. Le Client doit saisir son code Sécur'Pass chaque fois qu'il est invité à le faire sur l'application mobile de la Banque pour effectuer notamment les opérations suivantes :

- accéder au Service et, le cas échéant, à son compte de dépôt ;

- sécuriser l'accès et l'utilisation de certains services (ex : réinitialisation du mot de passe) ;

- valider des opérations de paiement (virements) et des opérations sensibles initiées depuis le Service ;

- valider des paiements par carte bancaire sur internet (e-commerce) ;

- s'authentifier, depuis le Service, lors de la souscription de produits et services commercialisés par la Banque par voie dématérialisée en ayant recours à un dispositif de signature électronique.

Sécur'Pass complète ou se substitue, le cas échéant, à la fonctionnalité Sécurisation des Opérations en Ligne (SOL) et aux modes d'authentification prévus par cette dernière, en permettant au Client de bénéficier de possibilités étendues.

L'enrôlement à Sécur'Pass est effectué par le Client par la saisie de certains numéros de sa carte bancaire en cours de validité et active, ou à défaut, de son adresse e-mail enregistrée par la Banque (sous réserve de disponibilité) ou 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 de sécurité. Afin d'utiliser Sécur'Pass, le Client doit également activer Sécur'Pass à partir de son Espace personnel de banque à distance accessible depuis l'application mobile. L'activation de Sécur'Pass

nécessite la saisie par le Client d'un code temporaire reçu sur le numéro de téléphone communiqué ainsi que d'un code Sécur'Pass qu'il a choisi.

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

Le choix, l'enregistrement, la modification, la réinitialisation et la conservation du code Sécur'Pass 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 personnel de banque à distance ou à ses moyens de paiement. La Banque n'a aucun accès à ce code Sécur'Pass.

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

Lors de l'utilisation de Sécur'Pass, la saisie du code Sécur'Pass 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, 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 et à la désinstallation préalable de l'application mobile de la Banque.

La suppression de Sécur'Pass 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, le Client devra procéder à un nouvel enrôlement.

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

5.3 Accès au compte de paiement par un prestataire de service d'initiation de paiement ou d'information sur les comptes

Dès lors que le Client autorise l'accès à son compte par un prestataire de service d'initiation de paiement ou d'information sur les comptes, ce prestataire doit disposer de l'agrément délivré par l'autorité compétente d'un Etat membre de l'Espace Economique Européen 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, à qui il communique, le cas échéant, ses identifiant et mot de passe, dispose de cet agrément ou est inscrit sur le registre concerné.

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 du Service.

5.4 Perte ou vol des identifiant et/ou mot de passe et/ou code d'authentification

Dès qu'il a connaissance de la perte, du vol, du détournement ou de toute utilisation frauduleuse de son identifiant et/ou de son mot de passe et/ou de son code d'authentification, le Client doit en informer sans tarder son agence ou le centre de relation clientèle qui procédera à la neutralisation de l'accès au Service. L'information devra être immédiatement confirmée par le Client par courrier recommandé avec avis de réception auprès de son

agence ou par courrier libre remis à l'agence contre décharge. En cas de contestation, la date de réception de cet écrit fera foi entre les parties.

La Banque recommande au Client de modifier son mot de passe dans les plus brefs délais.

5.5 Sécurisation des opérations en ligne

Dans le cadre de son abonnement au Service, le Client a accès à une fonctionnalité Sécurisation des Opérations en Ligne (ci-après « SOL ») dans l'environnement sécurisé du Service. SOL est utilisé pour les opérations sensibles (par exemple : accès au compte en ligne, ajout d'un compte bénéficiaire, enregistrement ou modification d'un ordre de virement permanent).

Dans le cadre de cette fonctionnalité :
- soit : la Banque envoie un code de contrôle par SMS vers le numéro de téléphone mobile désigné par le Client.

- soit le Client obtient un code de contrôle au moyen de sa carte bancaire et d'un lecteur d'authentification (calculette CAP).

Ce code de contrôle, reçu par SMS ou généré par lecteur CAP, doit être saisi par le Client, en complément du mot de passe, afin de réaliser les opérations sensibles.

Les Conditions Générales (CG) de SOL sont disponibles sur le site internet de la Banque.

6 - Responsabilités

6.1 Responsabilité de la Banque

La Banque s'engage à tout mettre en œuvre pour assurer au Client 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.

La Banque ne saurait être tenue pour responsable :
- en cas de non-respect par le Client des procédures d'utilisation du Service,
- en cas de divulgation par le Client de tout ou partie de ses éléments d'identification et d'authentification 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,
- lorsque les informations communiquées par le Client, lors de son adhésion ou de son utilisation du Service, s'avèrent inexactes ou incomplètes,
- en cas d'interruption des prestations pour des raisons résultant de la force majeure, du cas fortuit ou du fait d'un tiers,
- en cas de connexion du Client à un autre site que le site légitime et sécurisé de la Banque (https + adresse habituelle).
- 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, y compris de l'application mobile de la Banque. La Banque n'est pas responsable 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 suite à un mauvais fonctionnement du matériel du Client ou du réseau de télécommunications.

La Banque n'est pas responsable des conséquences résultant d'un défaut de sécurité (matériel ou logiciel, antivirus) du terminal de connexion (ordinateur, terminal mobile…) utilisé par le Client n'ayant pas détecté, notamment, l'intrusion d'un virus informatique.

La Banque dégage sa responsabilité des difficultés associées au contrat passé entre le Client et son fournisseur d'accès.

La Banque demeure étrangère à tout litige pouvant survenir entre le Client et :
- tout prestataire substitué, tant en ce qui concerne la facturation des coûts des transmissions que le bon fonctionnement du réseau téléphonique ;
- le prestataire de services fournisseur d'accès Internet en ce qui concerne l'accès aux différents sites Internet ;
- le fournisseur du matériel informatique (modem, ordinateur, logiciels, etc...) destiné à recevoir les informations par l'intermédiaire du téléchargement des écritures ;
- son prestataire de service d'initiation de paiement ou d'information sur les comptes.

De même, la responsabilité de la Banque ne saurait être engagée en raison des conséquences directes et indirectes liées aux mesures, quelles qu'elles soient, notamment de 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 se réserve le droit de limiter l'accès du Client aux seules fonctions de consultation ou de bloquer l'accès à Crédit Coopératif Direct, 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. La Banque met en place les moyens appropriés permettant au Client de demander à tout moment le déblocage du Service.

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.

6.2 Responsabilité du Client

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.

Le Client est tenu de sécuriser son ordinateur, sa tablette ou son téléphone mobile ainsi que les objets connectés associés, au moyen de solutions de sécurité de son choix (verrouillage du téléphone, logiciel anti-virus et anti-espion, pare-feu, logiciels de nettoyage …) et de maintenir ces dispositifs à jour en permanence. Il est conseillé au Client d'utiliser un téléphone mobile fonctionnant avec Android ou IOS et déconseillé d'utiliser les autres types de systèmes d'exploitation. Il lui est interdit de procéder au déverrouillage des systèmes d'exploitation.

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 de la Banque.

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 celui-ci à prendre toutes les dispositions utiles, notamment en

effaçant, dès la fin de sa consultation, les traces de sa navigation et en interdisant l'accès aux tiers non autorisés dans l'hypothèse du téléchargement de ces données bancaires vers un logiciel de gestion.

6.3 Responsabilité en cas d'opérations non autorisées

Conformément aux articles L.133-19 et L.133-20 du code monétaire et financier, lorsque les opérations de paiement non autorisées sont effectuées par l'intermédiaire des services de banque à distance, suite à la perte, au vol, au détournement ou à toute utilisation non autorisée de ce service ou des données qui lui sont liées, les règles spécifiques suivantes s'appliquent.

Avant la demande de blocage de l'instrument (appelé aussi mise en opposition) réalisée dans les conditions de l'article 5.4 :

- le Client supporte les pertes financières à hauteur de 50 euros en cas d'opération de paiement non autorisée consécutive à la perte ou au vol de ses dispositifs d'authentification et effectuée en utilisant les services de banque à distance pour l'émission d'ordres de virement en ligne ;

- le Client ne supporte aucune conséquence financière en cas :
  - de perte ou de vol des données de sécurité personnalisées ne pouvant être détecté par le Client avant le paiement du Client,
  - de perte de ces données 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.

La responsabilité du Client n'est pas engagée non plus lorsque l'opération non autorisée a été effectuée en détournant, à l'insu du Client, les données liées à l'instrument de paiement et en cas de contrefaçon de l'instrument.

Si la banque du bénéficiaire n'est pas située dans l'Espace Economique Européen, le Client supporte les pertes liées à l'utilisation de ses données de sécurité personnalisées avant l'information relative à la perte ou au vol dans la limite d'un plafond de 50 €.

Après la demande de blocage de l'instrument (appelé aussi mise en opposition), le Client ne supporte aucune conséquence financière.

De façon générale, les opérations non autorisées sont à la charge du Client en cas d'agissements frauduleux de sa part ou s'il n'a pas satisfait intentionnellement ou par négligence grave à son obligation générale de prudence rappelée dans la convention de compte en vigueur.

Sauf agissement frauduleux de sa part, le Client ne supporte aucune conséquence financière si l'opération de paiement non autorisée a été effectuée sans que la Banque n'exige une authentification forte du Client dans le respect de la procédure d'authentification forte mise en place par la Banque.

En particulier, la responsabilité du Client est engagée en cas de manquement à ses obligations de :
- prendre toute mesure pour conserver ses dispositifs d'authentification, préserver leur sécurité et leur confidentialité
- de demander sans tarder le blocage de l'instrument, dès qu'il a connaissance de la perte, du vol, du détournement ou de toute utilisation non autorisée de cet instrument ou des données qui lui sont liées.

7 - Preuve des opérations

Le Client s'engage à respecter l'ensemble des procédures d'accès, d'authentification et d'utilisation qui lui sont indiquées.

Lorsqu'un écrit, dûment signé par le Client, est une condition impérative d'exécution de l'opération envisagée, notamment pour souscrire aux produits et services offerts via le Service, le Client s'engage expressément à respecter cette condition. A défaut, la Banque sera fondée à ne pas tenir compte de l'opération demandée. Le Client accepte l'enregistrement informatique des connexions et opérations réalisées au cours de l'utilisation du Service. La preuve des opérations effectuées via le Service pourra être faite par toute forme d'enregistrements résultant des moyens de communication utilisés entre le Client et la Banque, dont les récapitulatifs des transactions établis par les systèmes informatiques de la Banque. De convention expresse, les parties reconnaissent que les enregistrements effectués par la Banque, quel qu'en soit le support, feront foi, sauf preuve contraire.

Lorsque le Client dialogue avec un conseiller, il autorise la Banque à enregistrer ses conversations téléphoniques, ainsi que celles des personnes auxquelles il aurait donné procuration et il admet ces enregistrements comme mode de preuve.

Le Client reconnaît que la reproduction sur tous supports, quels qu'ils soient, des entretiens téléphoniques entre lui et la Banque et toute personne à laquelle il aurait donné procuration, et/ou les interrogations ou ordres précédés de l'utilisation de l'identifiant, mot de passe et le cas échéant du Code/dispositif d'authentification du Client, dans le cadre du Service, sont réputés émaner de lui-même, ou de ses éventuels mandataires, et autorisés par le Client et constituent une preuve des opérations sollicitées et/ou réalisées, sauf preuve contraire.

Dans l'hypothèse où le Client refuserait l'enregistrement de ces entretiens téléphoniques, ou de faire précéder les interrogations ou ordres par l'identifiant, le mot de passe et le code d'authentification, la Banque sera fondée soit à lui refuser l'accès au Service, soit à lui interrompre le Service.

Ces supports ou leur reproduction seront conservés par la Banque pendant les délais réglementaires.

8 - Tarification

L'abonnement au Service est gratuit. Toutefois, l'utilisation de certains services, fonctionnalités ou opérations, depuis l'Espace personnel de banque à distance, peut donner lieu à tarification conformément aux conditions tarifaires en vigueur.

Tout défaut de paiement ouvre la faculté pour la Banque de suspendre les prestations sous réserve d'une information préalable au Client par lettre recommandée avec avis de réception. Cette suspension devient effective à l'issue d'un délai de 30 jours suivant l'envoi de cette lettre en cas de non-régularisation.

Le coût des communications téléphoniques et les frais divers directement facturés au Client, en particulier par les exploitants des réseaux de télécommunications, sont à sa charge.

9. Modifications des Conditions Générales et des conditions tarifaires

9.1 Modifications à l'initiative de la Banque

La Banque aura la faculté de modifier les conditions générales et les conditions tarifaires de ses services. A cet effet, la Banque communiquera au Client, au plus tard deux mois avant la date d'application envisagée, sur support papier ou sur tout autre support durable (par exemple, lettre, mention sur le relevé de compte ou information dans son Espace personnel de banque à distance), le projet de modification.

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, il peut résilier sans frais, avant la date d'application des modifications, le présent contrat régissant le Service, selon les modalités de l'article 10 ci-après. A défaut de

résiliation dans ce délai, les modifications lui seront opposables. La Banque peut également résilier le présent contrat dans les conditions de l'article 10.

9.2 Modifications imposées par des textes législatifs ou réglementaires

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

10 - Durée, résiliation ou suspension

Le présent contrat est conclu pour une durée indéterminée.

Le Client peut, comme la Banque, y mettre fin, par lettre recommandée avec avis de réception ou directement auprès de l'agence qui gère son compte, à tout moment, sans avoir à indiquer ni justifier du motif.

Lorsque la résiliation émane du Client, elle prendra effet dans le mois suivant la réception, par la Banque, du courrier recommandé envoyé par le Client.

La résiliation du contrat par la Banque doit respecter un préavis de deux mois.

Le présent contrat est résilié de plein droit et sans préavis en cas de décès du Client.

La résiliation du contrat entraîne la désactivation de l'ensemble des fonctionnalités et services disponibles dans l'Espace personnel de banque à distance du Client.

Par exception, pour le Client ayant bénéficié du service « e-Documents », l'accès à l'Espace personnel de banque à distance est maintenu même après la clôture du dernier contrat du Client, afin de permettre l'accès à l'historique des documents numériques dans les conditions spécifiques au service « e-Documents ».

Par ailleurs, la Banque se réserve le droit de suspendre l'accès ou l'exécution de tout ou partie des fonctionnalités du Service ou de résilier le présent contrat, sans aucun préavis, ni formalité si elle devait relever des faits laissant présumer la tentative ou l'utilisation frauduleuse de ces services, ou en cas de rupture des relations commerciales (non-paiement de facture, clôture du dernier contrat dont dispose le Client …), ce dont le Client serait immédiatement informé.

Tout ordre donné avant la date de résiliation est exécuté aux conditions et dates convenues.

Le Service pourra également être temporairement suspendu, en tout ou en partie, pendant des périodes courtes pour des raisons techniques et en vue de réaliser des prestations de maintenance ou d'actualisation du Service.

11 - « Messagerie Sécurisée Internet »

11.1 - Description du service

Après une connexion à son Espace personnel de banque à distance, le Client, a accès à une messagerie électronique avec la Banque dans l'environnement sécurisé du Service (ci-après, la « Messagerie Sécurisée Internet » ou « MSI »), conformément aux conditions et modalités ci-après.

11.2 - Accès à la messagerie Sécurisée Internet

La Messagerie Sécurisée Internet est accessible aux clients personnes physiques abonnés au Service.

Toute utilisation du Service sera réputée avoir été effectuée par le Client.

Le Client est informé qu'en résiliant son accès au Service, il met fin à l'accès à la Messagerie Sécurisée Internet. Dans ce cas, le Client perd définitivement l'accès aux messages conservés jusqu'alors dans sa MSI.

11.3 - Fonctionnalités de la Messagerie Sécurisée Internet

11.3.1 - Interlocuteurs du Client
La MSI permet au Client d'adresser, ou de recevoir, des messages électroniques en direction, ou en provenance, d'une ou plusieurs personnes du Réseau Crédit Coopératif dont la liste est définie par la seule Banque.

11.3.2 - Notification d'un nouveau message dans la Messagerie Sécurisée Internet
Sous réserve de la disponibilité de cette messagerie dans sa Banque et de la déclaration préalable d'une adresse électronique personnelle et valide, le Client peut recevoir une notification électronique des nouveaux messages parvenus dans sa Messagerie Sécurisée Internet.

La Banque n'est pas responsable de la saisie erronée de ses données personnelles par le Client, 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 suite à un mauvais fonctionnement du matériel du Client 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 personnel de Banque à distance (qui s'ajoute, éventuellement, à sa messagerie personnelle dès lors qu'il a fourni une adresse e-mail valide).

11.3.3 - Suppression des messages
Le Client a la possibilité de supprimer de la Messagerie Sécurisée Internet des messages électroniques émis ou reçus par lui. Dans ce cas, aucune restauration de ces messages ainsi supprimés ne sera possible ultérieurement.

11.3.4 - Limite à la capacité de stockage
La Messagerie Sécurisée Internet attribuée au Client 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 du Client.
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 du Client.

11.4 - Contenu des messages

11.4.1 - Règles d'utilisation de la Messagerie Sécurisée Internet
La MSI est exclusivement un service de dialogue entre le Client et des interlocuteurs Banque.
Le Client s'engage à n'utiliser la MSI que dans le cadre strictement limité à la relation bancaire défini par le Service. Aussi, le Client s'interdit de transmettre tout message, pièce jointe ou autre document qui n'aurait aucun lien direct, voire indirect avec l'objet du Service.

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. Par exception, la Banque

pourra éventuellement, par message MSI, informer préalablement le Client de l'augmentation du montant maximum de son autorisation de découvert dans les conditions de la convention de compte de dépôt.

Le Client est tenu soit d'effectuer ses opérations conformément aux dispositions du Service, soit de transmettre ses demandes à la Banque qui gère son compte.

Le Client devra faire un usage raisonnable de la MSI, notamment quant au contenu, à la fréquence des messages envoyés, 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 de la MSI.

La Banque se réserve le droit de mettre en demeure, par tous moyens, le Client de cesser une telle utilisation dans un délai de vingt-quatre heures. En cas de poursuite d'une utilisation déraisonnable par le Client, 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 Messagerie Sécurisée Internet ainsi supprimée.

11.4.2 - Traitement d'une demande formulée dans un message

En l'absence de réponse de l'interlocuteur dans un délai raisonnable, le Client est invité à contacter son agence par tout autre moyen.

La prise en compte des demandes de mise à jour des données et des informations personnelles du Client pourra être conditionnée par la Banque à la présentation par celui-ci des pièces justificatives correspondantes.

11.5 - Sécurité

Le Client 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 au Client via la MSI ; mais elle ne peut, compte tenu des aléas techniques, le garantir complètement. Il appartient, en conséquence, au Client de mettre en œuvre les mesures adéquates afin de préserver l'intégrité de son poste informatique. En tout état de cause, la Banque ne saurait être tenue responsable en cas de dommages causés au poste informatique du Client.

11.6 - Archivage des messages par le Client

La Banque rappelle au Client qu'il lui 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 son système informatique tous les documents ou messages stockés dans la Messagerie Sécurisée Internet, 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 par lui.

12. Protection des données à caractère personnel

Dans le cadre de la signature et de l'exécution des conditions générales et particulières du Service, et plus généralement de sa relation avec le Client, la Banque en tant que responsable de traitement recueille et traite des données à caractère personnel concernant :

- le Client et

- les personnes physiques intervenant dans le cadre de cette relation (mandataire, représentant légal, caution, contact désigné, préposé, bénéficiaire effectif, membre de la famille du Client…).

Si le traitement lié à une fonctionnalité du Service est fondé sur l'intérêt légitime de la Banque (ex : la catégorisation des dépenses prévue pour la gestion de budget), le Client peut à tout moment s'opposer à ce traitement et selon les modalités prévues dans la Notice d'information sur le traitement des données à caractère personnel.

Les informations expliquant
- pourquoi et comment ces données sont utilisées,
- combien de temps elles seront conservées,
- ainsi que les droits dont les personnes concernées disposent sur leurs données,

figurent dans la notice d'information de la Banque sur le traitement des données à caractère personnel.

Cette notice est portée à la connaissance des personnes concernées lors de la première collecte de leurs données. Elles peuvent y accéder à tout moment, sur le site internet de la Banque ((https://www.credit-cooperatif.coop/votre-banque/tarifs-et-informations-reglementaires/protection-donnees-personnelles) ou en obtenir un exemplaire auprès de leur Agence.

La Banque communiquera en temps utile les évolutions apportées à ces informations.

13. Réclamations – Médiation

En cas de difficultés concernant le Service, le Client peut obtenir de son Agence toutes les informations souhaitées, formuler auprès d'elle toute réclamation et/ou saisir par écrit le « Service Réclamation et Relation Client » 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 saisine du « Service Réclamation et Relation Client » de la Banque est effectuée par internet, à l'adresse suivante :

https://www.credit-cooperatif.coop/votre-banque/reclamation-mediation (coût de connexion selon fournisseur d'accès)

Ou par lettre envoyée à l'adresse suivante :

Crédit Coopératif – Service Réclamation et Relation Client - 12 boulevard Pesaro – CS 10002 – 92024 Nanterre cedex

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. Toutefois 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 pas 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 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.

Le Client peut saisir le médiateur de la Banque sur son site dédié : https://www.mediateur-fnbp.fr

ou en écrivant à :

Médiateur de la consommation auprès de la FNBP
20/22 rue Rubens
75013 PARIS

L'adresse postale du médiateur et les coordonnées du site internet du médiateur figurent aussi 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.

14. Démarchage bancaire et financier – Vente à distance

Lorsqu'un acte de démarchage précède la conclusion du présent contrat ou s'il a été conclu à distance, ce dernier peut, sous réserve de la demande préalable en ce sens par le Client, recevoir un commencement d'exécution avant l'expiration du délai de rétractation.

En tout état de cause, les opérations effectuées à l'initiative du Client vaudront accord de sa part sur un commencement d'exécution. Le commencement d'exécution ne prive pas le Client du droit de rétractation.

En cas de rétractation, et si le présent contrat a commencé à être exécuté,
- le Client devra restituer à la Banque les éventuelles sommes perçues et les éventuels moyens de paiement mis à sa disposition dans les meilleurs délais et au plus tard dans les trente (30) jours à compter de la réception de la notification.
- la Banque restituera au Client, dans les meilleurs délais et au plus tard dans les trente (30) jours, toutes les sommes qu'elle a reçues de ce dernier.

Ce délai commence à courir à compter du jour où le Client notifie à la Banque sa volonté de se rétracter.

Le Client sera tenu au paiement du prix correspondant à l'utilisation du produit ou service pour la période comprise entre la date de commencement d'exécution du contrat et de la date de rétractation, à l'exclusion de toute autre somme.

Les modalités de rétractation sont précisées aux conditions particulières du présent contrat.

15. Démarchage téléphonique

En application des dispositions du Code de la consommation, le Client est informé qu'il peut s'inscrire gratuitement sur une liste d'opposition au démarchage téléphonique.

Toutefois, malgré cette inscription, le Client peut être démarché par téléphone par la Banque lorsqu'il s'agit de sollicitations intervenant dans le cadre de l'exécution d'un contrat en cours et ayant un rapport avec l'objet de ce contrat, y compris lorsqu'il s'agit de proposer au consommateur des produits ou des services afférents ou complémentaires à l'objet du contrat en cours ou de nature à améliorer ses performances ou sa qualité.

16. Langue et droit applicables – Attribution de compétence

Le présent contrat est conclu en langue française. Le Client accepte expressément l'usage de la langue française durant les relations précontractuelles et contractuelles. Le présent contrat est soumis à la loi française et à la compétence des juridictions françaises.

17 - Agrément de la Banque et Autorités de contrôle

La Banque est un établissement de crédit agréé en France, contrôlé et supervisé par la Banque Centrale Européenne - Sonnemannstrasse 20, 60314 Frankfurt Am Main – Allemagne et par l'Autorité de Contrôle Prudentiel et de Résolution (ACPR) 4, place de Budapest CS92459 - 75436 Paris Cedex 09. La liste des établissements de crédit et plus généralement celle des prestataires de services de paiement habilités peut être consultée sur le site de l'ACPR à l'adresse suivante : https://acpr.banque-france.fr/proteger-la-clientele/vous-etes-un-particulier/verifier-si-un-professionnel-est-agree-immatricule.