CAISSE D'EPARGNE
ILE-DE-FRANCE

CONDITIONS GÉNÉRALES SPÉCIFIQUES DU SERVICE DE BANQUE À DISTANCE DIRECT ECUREUIL

(en vigueur au 13 janvier 2018)

1 - Description du service

Le service DIRECT ECUREUIL (ci-après « DE ») ou le « Service ») permet au Client d'accéder à des services bancaires, financiers et d'assurances, à partir de plusieurs canaux de communication (internet, téléphone fixe, mobile ou tablette). Il est ainsi possible au Client de réaliser à distance ses principales opérations.

Le Client peut également effectuer par l'intermédiaire de DE des opérations d'assurance sur ses produits d'assurance.
Les partenaires assureurs acceptent pour les opérations relatives à ces produits accessibles par DE l'ensemble des dispositions figurant aux articles 5 et 6 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.

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 à DE. De nouvelles fonctionnalités pourront progressivement être mises à disposition par la Banque. Le Client 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 en sera informé par tout moyen ainsi que des éventuelles modifications du coût de fonctionnement.

2 - Adhésion

Le service de DE est ouvert aux personnes physiques capables majeurs ou mineurs autorisés par leur représentant légal.

La détention d'un compte de dépôt ou d'un compte d'épargne par le Client n'est pas obligatoire pour avoir accès à DE.

En cas de compte joint, l'un et/ou l'autre titulaire peuvent être abonnés à DE. Chaque co-titulaire disposera de son propre numéro d'abonné et code confidentiel.

Les représentants légaux sont admis à effectuer des opérations sur les comptes de leurs enfants mineurs. Chaque représentant légal reconnaît que l'utilisation du numéro d'abonné et du code confidentiel, faite 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 à l'agence gestionnaire du compte. Le service Direct Ecureuil sera alors résilié par la Banque pour le ou les comptes du ou des mineur(s) concerné(s).

Le cas échéant, le Client peut conférer à un tiers une procuration spécifique sur un ou plusieurs de ses comptes, ce tiers devant lui-même adhérer au Service afin de disposer de ses propres identifiant et mot de passe.
Sont concernés les comptes ouverts à la date d'adhésion à DE et ceux ouverts ultérieurement.

3 - Spécificités de certaines fonctionnalités

a) Virements

Le Client peut effectuer des virements de l'un de ses comptes vers un autre de ses comptes et/ou vers un compte de tiers ouvert à la Caisse d'Epargne ou dans tout autre établissement de crédit, sous réserve :
- d'avoir signé préalablement une convention de compte de dépôt ou une convention de compte d'épargne auprès de la Banque,
- d'indiquer les coordonnées complètes du compte à débiter et à créditer, soit auprès de l'agence, soit dans le cadre de SOL ainsi que le montant concerné.

Mod. 01.18.000344 - 01/2018 - MAJ DJ : 11/2017 - Page : 1/8

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

Pour des raisons de sécurité, des plafonds sont appliqués par la Banque sur le montant des virements externes réalisés par l'intermédiaire du Service. La Banque est également susceptible d'appliquer des mesures complémentaires visant à protéger le Client de tout risque d'utilisation frauduleuse de son abonnement.

b) Versement par carte *(sous réserve de disponibilité)*
Le Client peut effectuer un versement par carte pour créditer un de ses comptes Caisse d'Epargne en utilisant une carte, dont il est titulaire, émise par un autre établissement. Seuls certains types de comptes sont éligibles à ces versements (compte de dépôt, Livret A, Livret B, Compte sur Livret, Livret Jeune, CEL, LDDS, LEP). Ces comptes peuvent être alimentés sous conditions de montant minimum de versement, de seuils et de plafonds minimum et maximum d'alimentation des comptes. Seules les cartes permettant une procédure d'authentification sont acceptées. Ces opérations de versement impactent le plafond de paiement de la carte utilisée.

c) Réservation d'espèces
Le Cient peut demander qu'une somme supérieure à celle habituellement remise lors d'un retrait au guichet soit tenue à sa disposition à l'agence de son choix, sous réserve du respect des consignes de sécurité imposées par la Banque, et moyennant un préavis. Le montant d'un retrait maximum sans préavis et la durée du préavis pour tout retrait d'un montant supérieur, seront indiqués au Client par son agence.

d) Opérations sur valeurs mobilières 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 fermes sur les marchés organisés français, à l'exception des marchés conditionnels, tous ordres sur les FCP et Sicav du Réseau des Caisses d'Epargne.

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 de DE.

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 Bourses.

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 titres et valeurs mobilières 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 ouvrés de leur réception, seront considérées comme approuvées. Si le Client souscrit au service « e-Documents », les avis d'opérés seront mis à disposition sur son espace personnel de DE. Le Client sera informé de cette mise à disposition dans sa MSI et par courriel dans sa messagerie personnelle à l'adresse e-mail indiquée lors de la souscription du service.

e) Oppositions sur chéquiers et cartes bancaires *(sous réserve de disponibilité)*
Toute opposition devra être confirmée dans les 48 heures par écrit adressé à la Banque.

f) Souscription aux services
Le Client peut souscrire dans le respect de la réglementation en vigueur applicable à certains services offerts par la Banque. La souscription effective du contrat 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.

g) Commande de chéquiers *(sous réserve de disponibilité)*
Le Client peut commander ses chéquiers sur DE. Le nombre total de chéquiers commandés quel que soit le canal (agence, GAB, DE) 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.

h) Messagerie Sécurisée Internet
Dans le cadre de son abonnement à DE, le Client a accès à une messagerie électronique dans l'environnement sécurisé de DE, la « Messagerie Sécurisée Internet » ci-après « MSI », dont les Conditions Générales d'Utilisation figurent à l'article 9 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.

i) Service de Règlement SEPAmail
Dans le cadre de son abonnement à DE, le Client a accès à un service de messagerie interbancaire dans l'environnement sécurisé de DE (le service « Règlement SEPAmail »). Ce service permet à un Client débiteur de recevoir une (des) demande(s) de règlement électronique adressée(s) par un Créancier via SEPAmail, en vue de son (leur) paiement(s) par virement SEPA, après l'acceptation par le Client. L'accès au Service est réservé aux titulaires d'un compte de dépôt, ouvert à la Caisse d'Epargne et permettant d'émettre des virements SEPA, et abonné à DE. Les Conditions Générales (CG) du service Règlement SEPAmail sont disponibles sur DE.

j) Gestion du budget *(sous réserve de disponibilité)*
Dans le cadre de son abonnement à DE par l'application mobile, le Client peut avoir accès à un service de gestion de budget gratuit permettant notamment de catégoriser automatiquement ses écritures dans des catégories de dépenses et de revenus.

Les écritures ainsi catégorisées sont disponibles pendant une période de 36 mois glissants à partir de la date de l'opération.

Le Client peut également accéder à des fonctionnalités d'agrégation étendues nécessitant l'acceptation préalable de conditions générales d'utilisation distinctes.

La résiliation de l'abonnement à DE entraîne la fermeture du service de Gestion du budget. L'ensemble des personnalisations et des catégorisations seront alors définitivement perdues.

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 DE 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 Service repose sur l'utilisation du réseau Internet. Le Client devra s'être procuré un accès au réseau internet avant la mise en place du Service.

Le Client accède à DE, par un matériel compatible (télécopieur, ordinateur multimédia, téléphone fixe, téléphone mobile ou tablette et objets connectés à ces derniers).

Pour l'accès aux fonctionnalités Internet, le Client devra disposer d'un logiciel compatible dont les fonctions JavaScript et Cookies sont activées.

Le Client fait son affaire personnelle de l'acquisition ou de la location, de l'installation et de la connexion, de l'entretien et de la garde du matériel et de tous moyens techniques, accès aux réseaux ou logiciels autres que ceux placés sous contrôle exclusif de la Banque. La Banque n'est pas responsable de l'évolution des logiciels, de leur mise à jour et du maintien des référencements.

5.2 - Modalités d'identification : numéro d'abonné et code confidentiel
Le Client accède aux services de DE, après son identification, par la composition d'un numéro d'abonné et d'un code confidentiel valables, quels que soient les moyens de connexion utilisés pour accéder à DE. Le numéro d'abonné est attribué au Client lors de la signature des conditions particulières lesquelles font partie intégrante de son contrat.

Pour permettre le premier accès à DE, la Banque attribue au Client un code confidentiel provisoire. Le Client est tenu de le modifier lors de sa première connexion. La Banque n'a pas accès au code confidentiel choisi par le Client.

Le numéro d'abonné et le code confidentiel attribués au Client sont personnels. Le Client prend toute mesure raisonnable pour préserver la sécurité de son numéro d'abonné et de son code confidentiel. L'utilisation de ses numéro et code est strictement personnelle. Le Client s'oblige à les tenir secrets et à ne les communiquer à quiconque. Ceci constitue une condition essentielle pour sécuriser les relations entre la Banque et le Client.

Ce code confidentiel peut être modifié à tout moment par le Client et à sa seule initiative ; la modification de ce code pour un canal vaut également pour les autres canaux d'accès à DE.

La Banque invite le Client à le faire fréquemment. Il est également conseillé au Client de ne pas choisir un code confidentiel 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 composition du code confidentiel, le dispositif d'accès aux services de DE devient inopérant. Dans ce cas, le service sera de nouveau accessible sur demande du Client auprès de l'agence qui gère son compte.

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 ou de l'enregistrement prévu par la règlementation en vigueur. Le Client est tenu d'informer la Banque de l'intervention d'un tel prestataire.

La Banque attire l'attention du Client sur les risques d'utilisation frauduleuse de ses données de sécurité personnalisées et des données liées à son compte lorsqu'il utilise les services d'un prestataire d'initiation de paiement ou d'information sur les comptes.

La Banque s'assure que les données de sécurité personnalisées (codes, authentification non rejouable) ne sont pas accessibles à d'autres personnes que celles autorisées par le Client, sauf si ce dernier ne respecte pas les préconisations mentionnées au présent article ou les préconisations relatives à SOL.

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

5.3 - Perte ou vol du code confidentiel
Dès qu'il a connaissance de la perte, du vol, du détournement ou de toute utilisation frauduleuse de son numéro d'abonné et de son code confidentiel, le Client doit en informer sans tarder son agence ou le centre de relation Clientèle qui procédera à la neutralisation de l'accès à DE. 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 code confidentiel dans les meilleurs délais.

5.4 - Sécurisation des opérations en ligne
Dans le cadre de son abonnement à DE, le Client a accès à une fonctionnalité Sécurisation des Opérations en Ligne (ci-après « SOL ») dans l'environnement sécurisé de DE. SOL est utilisé pour les opérations sensibles (création de RIB externe, réalisation de virement sur RIB enregistré au préalable dans l'abonnement à DE, modification de données personnelles du Client : numéro de téléphone mobile, adresse d'envoi des chéquiers, commandes de chéquiers ...). Les Conditions Générales (CG) de SOL sont disponibles sur DE.

5.5 - Secur'Pass *(sous réserve de disponibilité)*
Dans le cadre de son abonnement à DE, le Client a accès à l'application Secur'Pass.
Secur'Pass est un dispositif d'authentification forte permettant au Client, depuis une application installée sur son téléphone mobile (smartphone) :
- de sécuriser l'accès et l'utilisation de certains services ;
- de valider certaines opérations sensibles initiées depuis son espace personnel de Banque à distance (site internet DE ou application mobile DE) ;
- de valider des opérations de paiement à distance réalisées par carte bancaire (e-commerce) ;
- de s'authentifier lors de la souscription de produits et services commercialisés par la Caisse d'Epargne par voie dématérialisée en ayant recours à un dispositif de signature électronique.

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

Secur'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.

Afin d'utiliser Secur'Pass, le Client doit, au préalable, activer le service depuis son espace personnel de banque à distance, télécharger l'application sur son smartphone et suivre la procédure d'enrôlement. L'enrôlement à Secur'Pass nécessite que le Client soit détenteur d'une carte bancaire en cours de validité et active, d'un smartphone compatible et préalablement enrôlé, dont le numéro a été préalablement déclaré à la Banque en tant que téléphone de préférence.

Le changement de smartphone initialement enregistré nécessitera l'enrôlement du nouvel appareil.

Le choix, l'enregistrement, la modification, la réinitialisation et la conservation du code PIN associé à Secur'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 identifiants/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 PIN.

Il est conseillé au Client de changer son code PIN fréquemment, de ne pas choisir un code PIN simple aisément décelable par un tiers, et de ne pas choisir un code PIN 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 la banque à distance, ou le code associé à sa carte bancaire.

Le Client a la possibilité de désactiver le dispositif Secur'Pass à tout moment. En cas de cession de son smartphone, il lui appartient de veiller à la désactivation et à la désinstallation préalable de l'application.

La désactivation de Secur'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 Secur'Pass, le Client devra procéder à une nouvelle activation.

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

5.6 - Preuve des opérations sollicitées et/ou réalisées, dont l'enregistrement des conversations téléphoniques

Lorsqu'un écrit, dûment signé par le Client, est une condition impérative d'exécution de l'opération envisagée, notamment pour souscrire aux services offerts via DE, le Client s'engage expressément à respecter cette condition. A défaut, la Banque sera fondée à ne pas tenir compte de l'opération demandée. Il est néanmoins convenu entre les parties que la signature via l'utilisation du numéro d'abonné et du code confidentiel vaut signature manuscrite.

La preuve des opérations effectuées pourra être faite par toute forme d'enregistrements résultant des moyens de communication utilisés entre le Client et 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. La preuve des opérations effectuées pourra également être rapportée par tous moyens notamment par les récapitulatifs des transactions établies par les systèmes informatiques de la Banque.

Lorsque le Client dialogue avec un conseiller, il autorise la Banque à enregistrer ses conversations téléphoniques, ainsi que celles des personnes auxquelles il aurait confié ses codes d'accès 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 confié ses codes d'accès, et/ou les interrogations ou ordres précédés de l'utilisation de la double clé constituée du numéro d'abonné et du code confidentiel, dans le cadre des services de DE, sont réputés émaner de lui-même, ou de ses éventuels mandataires, et constituent une preuve des opérations sollicitées et/ou réalisées.

Dans l'hypothèse où le Client refuserait l'enregistrement de ces entretiens téléphoniques, ou de faire précéder les interrogations ou ordres par le numéro d'abonné et le code confidentiel, la Banque sera fondée soit à lui refuser l'accès à DE, soit à lui interrompre le service.

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

6 - Responsabilités

6.1 - Responsabilité de la Banque

La Banque s'engage à tout mettre en œuvre pour assurer au Client le bon fonctionnement de DE, 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 peut donner lieu à réparation.

La Banque ne saurait être tenue pour responsable :
- en cas de non-respect des procédures d'utilisation des services de DE,
- en cas de divulgation par le Client du code confidentiel 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 lors de l'adhésion du Client ou lors de l'utilisation de DE 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.

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.

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 DE, 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 de banque à distance.

6.2 - Responsabilité du Client

Le Client s'engage, notamment, au respect des conditions d'utilisation de DE 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.

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) :

- 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 euros.

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.

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 - Tarification

Le coût de l'abonnement est précisé dans les Conditions Tarifaires. A cet effet, le Client autorise la Banque à prélever sur le compte désigné aux Conditions Particulières toutes sommes dues au titre des prestations et services fournis.

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.

Il est rappelé que les services et/ou opérations sollicitées et/ou effectuées, notamment par l'intermédiaire de DE, peuvent donner lieu à tarification conformément à ces mêmes Conditions Tarifaires. Le coût des communications téléphoniques et les frais divers qui sont directement facturés au Client, en particulier par les exploitants des réseaux de télécommunications, sont à sa charge.

8 - Durée, résiliation ou suspension

L'accès à DE est ouvert pour une durée indéterminée. Le Client peut, 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. Celle-ci prendra effet dans le mois suivant la réception, par la Banque, du courrier recommandé envoyé par le Client.

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

Tout ordre donné avant la date de résiliation est exécuté aux conditions et dates convenues. En tout état de cause, l'accès est interrompu lors de la clôture du compte.

Par ailleurs, la Banque se réserve le droit de suspendre l'accès ou l'exécution de tout ou partie des services de DE ou résilier la présente convention, 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 compte ...), ce dont le Client serait immédiatement informé.

9 - Messagerie Sécurisée Internet

9.1 - Description du Service
L'abonné à DE (ci-après, « l'Abonné ») a accès à un service de messagerie électronique avec la Caisse d'Epargne dans l'environnement sécurisé de DE (ci-après, la « Messagerie Sécurisée Internet » ou « MSI »), conformément aux conditions et modalités ci-après.

9.2 - Accès à la messagerie Sécurisée Internet
Le Service est exclusivement accessible aux personnes physiques, capables majeurs ou mineurs autorisés par leur représentant légal, abonnées à Direct Ecureuil.

Toute utilisation du Service sera réputée avoir été effectuée par l'Abonné.

L'Abonné est informé qu'en résiliant son accès à DE, il met fin à l'accès à la Messagerie Sécurisée internet. Dans ce cas, l'Abonné perd définitivement l'accès aux messages conservés jusqu'alors dans sa MSI.

9.3 - Fonctionnalités du Service

9.3.1 - Interlocuteurs de l'Abonné
La MSI permet à l'Abonné d'adresser, ou de recevoir, des messages électroniques en direction, ou en provenance, d'une ou plusieurs personnes du Réseau de la Banque dont la liste est définie par la Banque.

9.3.2 - Notification d'un nouveau message dans la Messagerie Sécurisée Internet
Sous réserve de la déclaration préalable d'une adresse électronique personnelle et valide, l'abonné peut recevoir une notification électronique des nouveaux messages parvenus dans sa Messagerie Sécurisée Internet.

La Banque n'est pas responsable de la saisie erronée des données personnelles de l'Abonné, 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 de l'abonné ou du réseau de télécommunications.

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

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).

9.3.3 - Suppression des messages
L'Abonné 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.

9.3.4 - Limite à la capacité de stockage
La Messagerie Sécurisée Internet attribuée à l'Abonné 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'Abonné.

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'Abonné.

9.4 - Contenu des messages

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

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'Abonné est tenu soit d'effectuer ses opérations conformément aux dispositions de DE, soit de transmettre ses demandes à la l'agence qui gère son compte.

L'Abonné devra faire un usage raisonnable du service, en bon père de famille, 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.

La Caisse d'Epargne se réserve le droit de mettre en demeure, par tous moyens, l'Abonné de cesser une telle utilisation dans un délai de vingt-quatre heures. En cas de poursuite d'une utilisation déraisonnable par l'Abonné, la Banque se réserve le droit de résilier le service, sans que l'Abonné puisse prétendre à une quelconque indemnité, en raison notamment de la perte des messages contenus dans la Messagerie Sécurisée Internet ainsi supprimée.

9.4.2 - Traitement d'une demande formulée dans un message
En l'absence de réponse de l'interlocuteur dans un délai raisonnable, l'Abonné 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 de l'Abonné pourra être conditionnée par la Banque à la présentation par celui-ci des pièces justificatives correspondantes

9.5 - Sécurité
L'Abonné 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'Abonné via la MSI ; mais elle ne peut, compte tenu des aléas techniques, le garantir complètement. Il appartient, en conséquence, à l'Abonné 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 de l'Abonné.

9.6 - Archivage des messages par l'Abonné
La Banque rappelle à l'Abonné 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 l'Abonné des documents et messages susmentionnés qui n'auraient pas été correctement sauvegardés par lui.