

MOBILEbanking

Conditions particulières

Article 1. Disposition générale

Les Conditions Générales Bancaires de bpost banque régissent le Service MOBILEbanking. Les présentes Conditions Particulières complètent les Conditions Générales Bancaires en précisant les conditions et modalités propres au Service MOBILEbanking.

L'Abonné reconnaît avoir reçu les présentes Conditions Particulières et en avoir pris connaissance avant de souscrire le contrat d'abonnement MOBILEbanking. En souscrivant le contrat d'abonnement MOBILEbanking, l'Abonné accepte les présentes Conditions Particulières sans réserves.

Les Conditions Générales Bancaires, le contrat d'abonnement MOBILEbanking souscrit par l'Abonné et les présentes Conditions Particulières constituent le cadre contractuel du Service MOBILEbanking.

La Banque se réserve le droit de faire appel à des sous-traitants pour l'exécution du Service.

Article 2. Terminologie

Les termes suivants sont employés dans les présentes Conditions Particulières :

- Banque : bpost banque SA, rue du Marquis 1 bte 2 – 1000 Bruxelles.
- Abonné : la personne physique ayant souscrit le contrat d'abonnement MOBILEbanking et à laquelle le Service est accordé.
- Service : le service MOBILEbanking.
- Titulaire de (la) Carte : la personne physique au nom et au profit de laquelle la Banque a émis une Carte.
- Comptes Liés : les comptes à vue et comptes d'épargne ouverts auprès de la Banque et dont l'Abonné est (co-) titulaire ou mandataire, ou qui sont ouverts au nom d'une personne dont l'Abonné est le représentant légal.
- Procédures d'Activation et d'Accès : les techniques d'identification et de signature électroniques, plus précisément :
 - le Mot de Passe Unique et le Numéro d'Abonnement
 - le Numéro d'Abonnement, la Carte, le Code secret et le Lecteur de Carte
 - le Code de sécurité
 - la reconnaissance de l'empreinte digitale
 - la reconnaissance faciale

grâce auxquels l'Abonné peut activer le Service sur un Appareil et accéder au Service tel que décrit aux articles 6.1 et 6.2.

- Procédure de Signature : le système d'identification et de signature électroniques dans le cadre du Service au moyen de la Carte, Code secret et Lecteur de Carte, le Code de sécurité, la reconnaissance de l'empreinte digitale ou reconnaissance faciale permettant à l'Abonné de signer certains ordres transmis pendant l'utilisation du Service.

- Code de sécurité : un code d'identification personnel et confidentiel avec lequel l'Abonné s'identifie pour accéder au Service et/ou signer des ordres.
- Mot de Passe Unique : un code d'identification personnel et confidentiel grâce auquel l'Abonné peut activer le Service sur un Appareil conformément à l'article 6.1. Un mot de passe peut être demandé dans chaque bureau de poste. Un nouveau mot de passe est nécessaire pour chaque Appareil.
- Appareil : l'appareil grâce auquel l'Abonné reçoit accès au Service, à savoir un smartphone ou une tablette. Les exigences techniques auxquelles l'Appareil doit répondre peuvent être consultées sur www.bpostbanque.be.
- Carte : une carte de débit ou AccessCard émise par la Banque au nom de l'Abonné et liée à l'abonnement. Lorsqu'un Abonné est titulaire de plusieurs cartes, toutes les cartes sont liées à l'abonnement.
- Code secret : le code chiffré personnel et confidentiel lié à la Carte et permettant l'identification.
- Lecteur de Carte : le dispositif électronique permettant de s'identifier de manière sécurisée au moyen d'une signature électronique et de signer des ordres dans le cadre du Service.
- Empreinte digitale : les caractéristiques biométriques de l'Abonné, enregistrées par ce dernier dans le système d'exploitation de son Appareil. Cette fonction est installée sur l'Appareil par le fabricant de l'Appareil et/ou le concepteur du système d'exploitation prévu pour l'Appareil.
- Reconnaissance faciale : la reconnaissance des caractéristiques biométriques du visage de l'Abonné, enregistrées par ce dernier dans le système d'exploitation de son Appareil. Cette fonction est installée sur l'Appareil par le fabricant de l'Appareil et/ou le concepteur du système d'exploitation prévu pour l'Appareil.
- Numéro d'Abonnement : le numéro que la Banque attribue à l'Abonné afin de l'identifier. Pour les titulaires d'un abonnement PCbanking, le Numéro d'Abonnement est identique au numéro d'abonnement du service PCbanking.
- Compte Principal : le compte à vue lié à l'abonnement MOBILEbanking, tel que désigné par l'Abonné au moment de l'octroi du Service et sur lequel les éventuels frais relatifs au Service sont comptabilisés. Pour les titulaires d'un abonnement PCbanking, le Compte Principal est identique au compte de référence de l'abonnement PCbanking.
- Données de sécurisation personnelles : les moyens personnalisés que la Banque ou une autre banque met à la disposition des utilisateurs afin de s'authentifier. Chaque banque peut employer des moyens différents à cet effet.
- Autre banque : les institutions financières, autres que bpost banque, qui proposent et gèrent des comptes de paiement.

Article 3. Octroi du Service

Le Service peut être accordé à toute personne physique qui en fait la demande en qualité de (co-)titulaire ou de mandataire d'au moins un compte à vue dont il peut disposer seul et sans restriction de pouvoirs.

Les mineurs ne peuvent conclure un contrat d'abonnement MOBILEbanking que moyennant l'autorisation expresse de leurs représentants légaux.

La Banque n'est pas tenue de répondre positivement à une demande d'octroi du Service, ni de communiquer les motifs sous-jacents à une éventuelle décision négative.

Afin d'utiliser le Service, l'Abonné doit disposer d'un smartphone ou d'une tablette de type iOS ou Android. Les exigences techniques auxquelles l'Appareil doit répondre peuvent être consultées sur www.bpostbanque.be.

Article 4. Accès aux Comptes Liés

Dès que le Service est activé, tous les comptes à vue ou d'épargne dont l'Abonné est (co-)titulaire ou mandataire, ou qui sont ouverts au nom d'une personne dont l'Abonné est le représentant légal, deviennent des Comptes Liés.

Concernant les Comptes Liés dont l'Abonné ne peut disposer seul ou qu'avec restriction de pouvoirs, les services accessibles via le Service sont limités à la consultation de l'aperçu et de l'historique des mouvements sur le compte.

En tout état de cause, l'Abonné ne peut effectuer que les opérations compatibles avec les pouvoirs qu'il détient sur les Comptes Liés.

Article 5. Description des services accessibles via le Service

5.1. Le Service offre à l'Abonné la possibilité d'avoir accès à des services déterminés, tels que consulter des informations, exécuter des opérations, gérer des données ainsi qu'acheter certains produits et services proposés par la Banque.

Un aperçu détaillé est également disponible sur le site www.bpostbanque.be. La Banque peut toujours ajouter, modifier ou supprimer des fonctionnalités.

Pour les Abonnés mineurs, certains services ne sont pas accessibles, ou de manière limitée seulement.

5.2. Limites

Les limites suivantes sont applicables aux virements exécutés via le Service.

- Virements entre des Comptes Liés propres de l'Abonné :
Ces virements sont limités au solde disponible du Compte Lié à débiter.
- Virements au profit de comptes tiers :
Concernant les Abonnés majeurs, ces virements sont limités à un montant maximum de 1 000 € par jour et de 5 000 € par semaine. La limite par opération s'élève à 1 000 €. Concernant les Abonnés mineurs, ces virements sont limités à un montant maximum de 125 € par jour et de 125 € par semaine. La limite par opération s'élève à 125 €.

En tout état de cause, une opération n'est exécutée que si le solde du Compte Lié à partir duquel elle est exécutée est suffisant, compte tenu des opérations n'ayant pas encore été comptabilisées. De plus, une opération n'est exécutée que si et seulement si la nature du Compte Lié donneur d'ordre et les conventions applicables à ce compte autorisent l'opération.

5.3 Communication

Dans les limites autorisées par la loi et sans préjudice d'accords dérogatoires avec l'Abonné, un certain nombre d'informations, messages ou documents légaux, réglementaires ou contractuels seront communiqués aux titulaires d'un abonnement PCbanking et/ou MOBILEbanking exclusivement via ces deux canaux digitaux. L'Abonné s'engage à prendre régulièrement connaissance des informations, messages et documents communiqués.

Article 6. Activation – Accès – Signature

6.1. Activation du Service

Afin d'accéder au Service, l'Abonné doit tout d'abord installer l'application requise sur son Appareil. L'Abonné doit ensuite s'enregistrer sur l'application installée sur son Appareil. Pour ce faire, l'Abonné utilise :

- son Numéro d'Abonnement et le Mot de Passe Unique ; ou
- son Numéro d'Abonnement, la Carte, ainsi que le Code secret y associé et le Lecteur de Carte (pas applicable aux Abonnés mineurs).

Lors de cette première connexion, l'Abonné complète son profil et choisit un Code de sécurité. Le Code de sécurité peut être modifié à tout moment au moyen du Service.

Si la fonctionnalité de lecture de l'empreinte digitale ou reconnaissance faciale est disponible sur son Appareil, l'Abonné peut activer cette fonction lors de sa première connexion et en faire usage comme moyen d'identification pour sa connexion au Service. Si l'Abonné n'active pas cette fonction lors de sa première connexion, il pourra, s'il le souhaite, l'activer par la suite. L'Abonné peut à tout moment désactiver cette fonction sans impact sur les autres procédures d'Accès. La Banque fait uniquement usage de la lecture de l'empreinte digitale ou reconnaissance faciale comme moyen pour l'Abonné d'obtenir l'accès au Service. La Banque n'enregistre aucune information sur l'empreinte digitale ou les caractéristiques du visage. Pour plus d'information, la Banque renvoie au fabricant de l'Appareil concerné.

Un Abonné peut activer le Service sur un maximum de 8 Appareils différents.

Les Abonnés peuvent supprimer tout Appareil de leur abonnement MOBILEbanking auprès de n'importe quel bureau de poste.

6.2. Accès

Lors de tout accès au Service, l'Abonné s'identifie au moyen de son Code de sécurité, ou de son empreinte digitale ou reconnaissance faciale, si la fonctionnalité est activée.

Après trois saisies erronées consécutives du Code de sécurité, la Banque bloque automatiquement l'accès de l'Appareil concerné au Service. L'Abonné est alors tenu de prendre contact avec POSTINFO au

numéro 022/012345 du lundi au vendredi de 8h à 12h30 et de 13h à 18h, et le samedi de 9h à 13h.

Après plusieurs tentatives infructueuses d'identification au moyen de l'empreinte digitale ou de la reconnaissance faciale, l'Abonné devra suivre les règles et instructions de la plateforme iOS ou Android utilisée. L'Abonné peut toujours se connecter via son Code de sécurité.

6.3. Signature des ordres

La signature des ordres se fait intégralement par voie électronique. Après avoir rempli l'ordre, l'Abonné confirme l'opération. Il peut être invité à cet effet à signer certains ordres via la Procédure de Signature.

La signature, telle que décrite à l'alinéa précédent, constitue une preuve valable et décisive de l'accord de l'Abonné quant à l'existence et au contenu de l'ordre.

Article 7. Service d'information sur les comptes et service d'initiation de paiement

7.1. Le Service MOBILEbanking offre à l'Abonné la possibilité de recourir aux services de paiement suivants :

- service d'information sur les comptes ;
- service d'initiation de paiement.

Ces services de paiement sont uniquement disponibles lorsque le Service a été installé sur un smartphone.

L'utilisation de ces services est toujours subordonnée au consentement de l'Abonné, tel que décrit ci-après. Dès que la connexion est établie avec une autre banque, la Banque s'identifiera et communiquera de manière sécurisée.

Les informations relatives au traitement des données à caractère personnel assuré dans ce cadre se trouvent dans la Déclaration Vie Privée de la Banque.

Service d'information sur les comptes

L'Abonné peut ajouter un ou plusieurs comptes de paiement (généralement de type compte à vue), ouverts auprès d'une autre banque et dont il est (co-)titulaire ou mandataire, à son relevé de compte dans l'application MOBILEbanking et y consulter les informations y afférentes. Les comptes concernés doivent pouvoir être consultables en ligne auprès de l'autre banque. La possibilité d'ajouter ou non des comptes est toujours soumise aux règles et conditions en vigueur auprès de l'autre banque.

L'Abonné peut consulter le solde des comptes ajoutés et l'historique des opérations exécutées.

L'Abonné souhaitant recourir à ce service doit donner son consentement à la Banque quant à l'obtention des données disponibles de ce(s) compte(s) ouvert(s) auprès de l'autre banque. Dans ce cas, il donne son consentement dans l'application MOBILEbanking.

L'Abonné a toujours la possibilité de retirer son consentement en supprimant les comptes ajoutés de son relevé de compte dans l'application.

Après recueil du consentement, la Banque établit la connexion avec l'autre banque et l'Abonné doit s'authentifier auprès de celle-ci à l'aide des données de sécurisation personnelles obtenues de cette autre

banque. L'autre banque décide de la durée de validité de l'accès sans nécessiter de nouvelle authentification. Cette durée peut varier d'une banque à l'autre, la durée maximale étant fixée à 90 jours. Au terme de ce délai, l'Abonné devra à nouveau se connecter et s'authentifier, faute de quoi ses données ne seront plus mises à jour.

Service d'initiation de paiement

L'Abonné peut initier un ordre de paiement sur les comptes à vue qu'il détient auprès d'une autre banque, pour autant qu'il les ait ajoutés à son relevé de compte dans l'application MOBILEbanking.

Dès qu'un Abonné souhaite initier un paiement depuis un compte détenu auprès d'une autre banque, il devra y donner son consentement explicite à la Banque.

L'Abonné indique toutes les données nécessaires à l'initiation du paiement sur l'écran prévu à cet effet, avant d'autoriser la Banque à établir la connexion avec l'autre banque et à transmettre l'ordre de paiement.

La Banque fait basculer l'Abonné dans l'environnement de banque en ligne de l'autre banque, où il devra s'identifier et s'authentifier à l'aide des données de sécurisation personnelles obtenues de cette autre banque. Ensuite, la Banque transmet toutes les données de l'ordre de paiement à l'autre banque.

L'autre banque exécute l'opération conformément aux conditions d'exécution exposées dans le contrat-cadre conclu entre l'Abonné et l'autre banque.

La Banque informe l'Abonné quant à la réussite ou non de l'initiation de l'ordre de paiement sur la base des renseignements fournis par l'autre banque.

7.2. L'Abonné peut avoir accès, par l'intermédiaire d'un prestataire de services tiers, à certaines informations des comptes liés (services d'information sur les comptes) et/ou ordres de paiement sur ces comptes transmis à la Banque (services d'initiation de paiement). Le prestataire de services tiers (fournisseur de services d'information sur les comptes ou d'initiation de paiement) établit à cet effet, moyennant le consentement explicite de l'Abonné, une connexion avec l'environnement de banque en ligne de la Banque. L'Abonné devra ensuite se connecter et s'authentifier au moyen des données de sécurité personnelles reçues de la Banque ou acceptées par celle-ci (p. ex. itsme). Lorsqu'un ordre de paiement est donné par l'intermédiaire d'un prestataire de services d'initiation de paiement, la Banque l'exécute selon les conditions définies dans le contrat-cadre entre l'Abonné et la Banque.

Article 8. Obligations et responsabilité de l'Abonné

8.1. L'Abonné est tenu d'utiliser le Service conformément aux conditions qui en régissent l'émission et l'utilisation. Il est notamment tenu de respecter strictement toutes les instructions relatives aux procédures d'activation, d'accès et d'utilisation, ainsi que les normes de sécurité décrites dans les présentes Conditions Particulières.

8.2. L'Abonné ne peut annuler les virements qu'il a exécutés dans le cadre du Service, à l'exception des virements dont l'exécution est programmée à une date ultérieure. Ces virements peuvent être

annulés au plus tard le jour ouvrable bancaire précédant la date ultérieure, telle que programmée.

8.3. L'Abonné est tenu de prendre toutes les mesures de précaution raisonnables afin de garantir la sécurité des Procédures d'Activation, d'Accès et de Signature, d'en protéger la nature personnelle et confidentielle et de prévenir tout danger lié à une utilisation non autorisée du Service. Il s'engage notamment à ne pas les communiquer à des tiers, à ne pas les mettre à la disposition de tiers et à ne pas les mettre à la portée de tiers.

L'Abonné qui a choisi d'utiliser son empreinte digitale ou la reconnaissance faciale comme moyen d'identification lors de sa connexion au Service s'assure que seules ses propres empreintes digitales ou faciales sont enregistrées sur son Appareil. Il ne fera enregistrer aucune empreinte digitale ou faciale autre que la sienne. Avant d'activer la fonction de lecture d'empreintes digitales ou la reconnaissance faciale pour l'utilisation de l'application MOBILEbanking, l'Abonné s'engage à effacer de son Appareil toutes les empreintes digitales ou faciales liées à d'autres personnes. L'Abonné est responsable de toutes les conséquences liées au non-respect de cette obligation.

L'Abonné est tenu de prendre toutes les mesures de précaution raisonnables afin de prévenir toute utilisation illicite de son Appareil. Il veille à ce que son smartphone/sa tablette soit sécurisé(e).

À cet effet, l'Abonné respecte notamment les mesures de sécurité visées au point 8.4.

8.4. Mesures de sécurité :

- Mémorisez votre Code de sécurité. Ne le notez nulle part sous une forme facilement reconnaissable, sur quelque support que ce soit. Ne le communiquez pas à des tiers, ni à des membres de votre famille, à votre banque ou à la police.
- Ne notez jamais votre Code de sécurité sur ou dans l'Appareil, pas même sous une forme codée.
- Soyez discret lors de la saisie de votre Code de sécurité.
- Choisissez immédiatement un autre Code de sécurité lorsque vous soupçonnez que son caractère confidentiel n'est plus garanti. Le cas échéant, avertissez la Banque (cf. point 5).
- Ne laissez pas l'Appareil, ainsi que les moyens d'activation, d'accès et de signature sans surveillance (par ex. : sur votre lieu de travail, dans votre véhicule, à votre hôtel ou dans tout autre lieu accessible au public).
- Fermez la session en appuyant sur « Déconnexion » dès qu'elle est terminée. Ne laissez pas l'Appareil sans surveillance pendant la session, pour quelque motif que ce soit.
- Ne permettez pas à des tiers d'utiliser votre Appareil tant que vous êtes connecté au Service.
- Veillez à être l'utilisateur exclusif de l'Appareil lorsque vous activez la fonction de lecture de l'empreinte digitale et à n'enregistrer que vos propres empreintes digitales ou faciales.

8.5. L'Abonné est tenu d'informer POSTINFO dès qu'il a connaissance de la perte, du vol, de l'utilisation illicite ou non autorisée de sa Procédure d'Activation, d'Accès ou de Signature et/ou,

le cas échéant, de son Appareil, afin de bloquer l'accès au Service via l'Appareil concerné.

L'Abonné peut également supprimer l'Appareil concerné de son abonnement MOBILEbanking auprès de n'importe quel bureau de poste.

Si nécessaire, l'Abonné peut bloquer son abonnement MOBILEbanking. À cet égard, l'Abonné doit tenir compte du fait que son abonnement PCbanking sera bloqué par la même occasion.

POSTINFO est accessible par téléphone au numéro 022/012345 du lundi au vendredi de 8h à 12h30 et de 13h à 18h, et le samedi de 9h à 13h.

Lorsque les faits sont constatés en dehors des jours et heures d'accessibilité de POSTINFO, l'Abonné est tenu de notifier lesdits faits dès que possible.

En cas de perte, de vol ou (de risque) d'utilisation illicite ou non autorisée de la Carte et du Code secret, l'Abonné est tenu d'en informer immédiatement Card Stop au numéro 078/170.170. Il agit conformément aux dispositions des conditions particulières applicables à la Carte concernée.

L'Abonné signale par ailleurs toute comptabilisation sur les extraits de compte résultant d'une opération non autorisée ou incorrecte exécutée via le Service, ainsi que toute irrégularité constatée sur les extraits de compte.

L'Abonné prend toutes les mesures raisonnables pour constater (le risque de) perte, vol, utilisation illicite ou non autorisée.

L'Abonné est tenu de porter plainte auprès de la police dans un délai de vingt-quatre (24) heures à compter de la constatation des faits.

8.6. L'Abonné est responsable de toute perte liée aux opérations non autorisées découlant de l'utilisation de ses Procédures d'Activation, d'Accès ou de Signature perdues, volées ou utilisées illicitement, et ce, à compter du moment où lesdites Procédures sont en sa possession jusqu'à la notification visée au point 5, avec un maximum de 50 €. Le montant maximum de 50 € ne s'applique toutefois pas et l'Abonné supporte toutes les pertes lorsque celui-ci a agi frauduleusement, intentionnellement ou avec négligence grave.

La Banque se réserve le droit de considérer notamment comme une négligence grave, eu égard aux circonstances de fait, le non-respect d'une ou de plusieurs des obligations contenues aux points 1, 3, 4, 5 et 9 de cet article, sans préjudice du droit de l'Abonné de faire appel au pouvoir d'appréciation du juge conformément à la loi.

Après avoir procédé à la notification visée au point 5, l'Abonné n'est plus responsable des conséquences financières découlant de l'utilisation des Procédures d'Activation, d'Accès et de Signature perdues, volées ou obtenues illicitement, sauf agissement frauduleux dans son chef.

L'Abonné ne supporte aucune perte s'il n'a pas pu constater la perte, le vol ou l'utilisation illicite avant que le paiement ait eu lieu, sauf lorsqu'il a agi frauduleusement ou intentionnellement ou si la perte est due à des actes ou des manquements d'un employé, d'un agent de la Banque ou d'une entité à qui des activités ont été externalisées.

8.7 L'Abonné qui constate des irrégularités ou des opérations non autorisées sur des comptes détenus auprès de l'autre banque et ajoutés à l'application MOBILEbanking doit s'adresser à son autre banque en vue d'obtenir un éventuel remboursement, même si ces

opérations ont été initiées dans l'application MOBILEbanking. La Banque n'intervient pas dans ces litiges.

Si l'Abonné constate la perte, le vol ou l'utilisation illicite de ses données de sécurisation personnelles obtenues de l'autre banque afin de s'authentifier, il doit agir conformément aux dispositions du contrat qu'il a conclu avec cette autre banque.

8.8 La Banque met régulièrement à disposition une nouvelle version de l'application MOBILEbanking (« mise à jour »). L'Abonné s'engage à mettre à jour l'application MOBILEbanking de son Appareil dès que bpost banque met une mise à jour à disposition. bpost banque n'est en aucun cas responsable des conséquences du non-respect de la présente obligation.

Lors de chaque mise à jour, l'Abonné recevra, avant l'installation, un message contenant une description des modifications. L'Abonné s'engage à prendre connaissance de ces modifications. L'installation de la nouvelle version par l'Abonné implique l'acceptation des modifications apportées.

Article 9. Obligations et responsabilité de la Banque

9.1. La Banque a mis en place, pour le Service, des systèmes conformes aux normes technologiques actuelles et prend des mesures raisonnables pour en garantir la sécurité. Elle prend les mesures nécessaires afin de garantir la confidentialité des moyens personnels d'Activation, d'Accès et de Signature des Abonnés.

Si la Banque constate une fraude présumée ou effective concernant l'abonnement d'un Abonné, elle l'en avertira par téléphone ou par tout autre moyen de communication adapté. À cet égard, la Banque ne demandera jamais de communiquer le code secret de la carte de débit ou un code créé avec la carte de débit ou tout autre code secret ou moyen de sécurité personnel.

La Banque avertit également ses clients par l'intermédiaire des communications générales sur son site web ou des messages généraux dans PCbanking ou MOBILEbanking afin d'attirer leur attention sur d'éventuelles fraudes (p. ex. phishing).

9.2. La Banque enregistre les données essentielles de chaque opération exécutée dans le cadre du Service, au moment de ladite exécution. Ces enregistrements sont conservés par la Banque au moins dix (10) ans à compter de l'exécution des opérations concernées et peuvent être reproduits sous forme lisible sur n'importe quel support d'informations type. Lorsque l'Abonné nie avoir autorisé une opération exécutée dans le cadre du Service ou soutient que l'opération n'a pas été correctement exécutée, il appartient à la Banque de démontrer que l'opération a été authentifiée, qu'elle a été correctement enregistrée et comptabilisée, et qu'elle n'a pas été influencée par un problème technique ou toute autre défaillance.

La Banque apporte cette preuve de manière valable en produisant les enregistrements relatifs aux opérations litigieuses, sans préjudice de la preuve contraire apportée par l'Abonné.

Lorsque l'Abonné soutient qu'une opération n'a pas été correctement exécutée, la production desdits enregistrements par la Banque constitue une preuve décisive de la correcte exécution de l'opération.

9.3. La Banque met tout en œuvre afin de garantir autant que possible la continuité du Service. La Banque se réserve toutefois le droit d'interrompre, si nécessaire et sans indemnité, le Service pendant un délai raisonnable, notamment pour l'entretien ou l'installation de nouvelles versions ou mises à jour des systèmes et appareils.

9.4. Pour autant que l'Abonné respecte l'intégralité de ses obligations, la Banque est responsable :

- de l'inexécution ou de l'exécution incorrecte d'ordres que l'Abonné a correctement transmis, dans le cadre et suivant les normes d'utilisation du Service, via des Appareils répondant aux exigences techniques fixées par la Banque ;
- des ordres qui ont été exécutés sans l'autorisation de l'Abonné.

En cas de responsabilité de la Banque, cette dernière est tenue, selon le cas :

- de rembourser le montant de l'opération inexécutée ou incorrectement exécutée et, le cas échéant, de remettre les Comptes Liés concernés dans l'état où ils se trouveraient si l'opération incorrectement exécutée n'avait pas eu lieu ;
- de rembourser le montant de l'opération non autorisée et, le cas échéant, de remettre les Comptes Liés concernés dans l'état où ils se trouveraient si l'opération non autorisée n'avait pas eu lieu, en ajoutant le cas échéant les intérêts produits sur ce montant ;
- de prendre en charge les éventuelles conséquences financières de l'opération non autorisée, notamment les frais engagés par l'Abonné pour déterminer le montant du dommage à réparer.

La date de valeur du remboursement d'un montant d'une transaction sur un compte à la suite de l'alinéa précédent ne sera pas ultérieure à la date à laquelle le montant a été initialement débité du compte concerné.

9.5. Si l'Abonné conteste une opération exécutée sur un compte détenu auprès d'une autre banque et initiée dans l'application MOBILEbanking, il doit s'adresser à cette autre banque. L'autre banque constitue en effet le seul point de contact pour l'Abonné. La Banque n'intervient pas dans les litiges opposant l'autre banque à l'Abonné. La Banque et l'autre banque sont chacune responsables de la partie des opérations de paiement dont elles ont la maîtrise. Le cas échéant, l'autre banque prendra contact avec la Banque afin de déterminer ensemble leur part de responsabilité respective. Dans ce cadre, la Banque devra apporter la preuve que l'opération en question a été authentifiée et dûment enregistrée, et qu'elle n'a pas été affectée par une déficience technique ou autre des systèmes placés sous son contrôle. La Banque devra démontrer qu'elle a correctement initié l'ordre de paiement auprès de l'autre banque et que celle-ci a effectivement reçu ledit ordre.

Lorsqu'un ordre de paiement a été initié par l'Abonné par l'intermédiaire d'un prestataire de services d'initiation de paiement, la Banque indemniserà le client pour la transaction non exécutée ou incorrectement exécutée et, le cas échéant, remettra le compte dans l'état dans lequel il se serait trouvé si la transaction de paiement incorrecte n'avait pas eu lieu et ce, sans préjudice des dispositions de l'article 8. Le cas échéant, la Banque s'adressera au prestataire de services d'initiation de paiement qui devra fournir la preuve nécessaire que l'ordre a été initié et reçu correctement par la Banque.

9.6. La Banque ne peut être tenue responsable des dommages résultant directement ou indirectement d'un dysfonctionnement du dispositif de l'Abonné ou du service de télécommunications fourni par des tiers, ou encore d'une interruption du Service pour des motifs indépendants de la volonté de la Banque.

Article 10. Propriété intellectuelle

Tous les droits de propriété intellectuelle sur l'application MOBILEbanking et sur l'ensemble des informations, documents, publications concernant cette app sont détenus par la Banque et/ou, le cas échéant, par ses fournisseurs. L'Abonné se voit accorder un droit d'utilisation personnel, non exclusif et non transmissible pour toute la durée du contrat relatif au Service.

L'Abonné s'engage à respecter ces droits et à s'abstenir de toute violation de ceux-ci. Cela implique notamment de ne pas copier, manipuler, compiler ou modifier, diffuser ou mettre à la disposition de tiers de quelque façon que ce soit des logos, marques, logiciels ou tout autre élément de l'application MOBILEbanking sur lesquels sont détenus de droits de propriété intellectuelle.

Article 11. Tarifs et frais

La Banque se réserve le droit de tarifier le Service et les opérations exécutées dans le cadre de celui-ci.

Tous les frais liés au Service sont renseignés dans la Liste des Tarifs, telle que visée à l'article 21 des Conditions Générales Bancaires et communiquée à l'Abonné conformément aux dispositions du présent article.

L'Abonné est tenu de supporter tous les frais liés à son Appareil (achat, installation et fonctionnement), ainsi que les frais de connexion à Internet et les frais de télécommunications.

Article 12. Blocage et cessation du Service

La Banque peut à tout moment et sans avertissement bloquer le Service en cas de motifs justifiés, comme lorsque la sécurité du Service est compromise ou que l'on suspecte un usage non autorisé ou abusif. La Banque informe l'Abonné, si possible avant le blocage ou au plus tard immédiatement après. Cette fourniture d'information n'est pas exigée lorsque cet objectif interférerait avec des préoccupations légitimes de sécurité ou serait lié à une loi ou réglementation. Dès lors que les raisons du blocage n'existent plus, le blocage est levé.

L'Abonné ou la Banque peuvent à tout moment mettre fin unilatéralement au Service, sans devoir fournir un quelconque motif. L'Abonné est tenu de clôturer le Service auprès d'un bureau de poste.

Lorsque la Banque décide de mettre fin à l'abonnement, elle est tenue de notifier à l'Abonné un délai de préavis d'au moins deux (2) mois.

La Banque peut, pour des motifs justifiés, résilier l'abonnement avec effet immédiat et en informer l'Abonné.

La Banque se réserve le droit de bloquer l'accès au Service en cas de risque d'abus ou de fraude. En cas de cessation du Service, la redevance annuelle est remboursée proportionnellement à compter du mois qui suit la date de la cessation.

Le Service prend automatiquement fin lorsque plus aucun compte à vue n'est lié à l'abonnement.

Article 13. Modification

La Banque a la possibilité de modifier à tout moment les présentes Conditions Particulières unilatéralement. L'Abonné en est informé soit par écrit, soit par le support durable mis à sa disposition et auquel il peut accéder, au moins deux (2) mois avant l'entrée en vigueur de la modification. À défaut de réaction de l'Abonné dans ce délai de deux (2) mois, il est réputé avoir accepté la modification.

Article 14. Plaintes et litiges

Nonobstant l'article 8.5 des présentes Conditions, toute contestation relative à une opération non autorisée ou incorrectement exécutée dans le cadre du Service doit être signalée immédiatement par écrit, dès la constatation de celle-ci sur les extraits de compte et au plus tard dans les treize (13) mois à compter de la date de débit ou de crédit de l'opération contestée. À défaut de réclamation communiquée dans ce délai, l'opération est réputée avoir été correctement exécutée et approuvée.

Les réclamations en relation avec la Carte ou des services qui y sont liés peuvent être introduites :

- par le formulaire de contact en ligne sur www.bpostbanque.be
- par courrier adressé à Postinfo – bpost banque, Boulevard Anspach 1 à 1000 Bruxelles
- par e-mail adressé à plaintes.bpostbanque@bpost.be
- par téléphone au numéro 022/012345

Si le client n'est pas d'accord avec la solution proposée, il peut également s'adresser au service Customer Services de bpost banque, rue du Marquis 1 bte 2 à 1000 Bruxelles, ou par e-mail : quality@bpostbanque.be.

Après avoir épuisé toutes les possibilités offertes au sein de la Banque, le Titulaire de la Carte ou du compte peut demander l'intervention de l'Ombudsfin – Service de médiation des services financiers, par courrier adressé à North Gate II, boulevard du Roi Albert II 8 bte 2 à 1000 Bruxelles, par téléphone 02/545.77 70, par e-mail à l'adresse Ombudsman@ombudsfin.be ou par le formulaire de contact en ligne sur le site Internet de ce service www.ombudsfin.be.

Les plaintes peuvent également être soumises au SPF Économie, Direction générale de l'inspection économique, par courrier adressé à North Gate II, boulevard du Roi Albert II 16 à 1000 Bruxelles, par téléphone au 02/277 54 84, par e-mail à l'adresse eco.inspec fo@economie.fgov.be ou par le formulaire de contact en ligne sur le site Internet de ce service www.economie.fgov.be.

PCbanking

Conditions particulières

Article 1. Stipulation générale

Les Conditions Générales Bancaires de bpost banque régissent le Service PCbanking.

Les présentes Conditions Particulières complètent ces Conditions Générales Bancaires en précisant les conditions et modalités propres au Service PCbanking.

L'Abonné reconnaît avoir reçu et pris connaissance des présentes Conditions avant la signature de la convention d'abonnement. En signant la convention d'abonnement, il y adhère sans réserve.

Les Conditions Générales Bancaires, la convention d'abonnement signée par l'Abonné, les présentes Conditions Particulières et le manuel d'utilisation, forment le cadre contractuel du Service PCbanking.

La Banque se réserve le droit, pour l'exécution du Service, de faire appel à des sous-traitants.

Article 2. Terminologie

Dans les présentes Conditions Particulières, les termes suivants sont utilisés:

- Banque : bpost banque SA, Rue du Marquis 1 boîte 2 - 1000 Bruxelles.
- Abonné : la personne physique à qui a été attribué le Service et qui a signé la convention d'abonnement.
- Titulaire de carte : la personne physique au nom de laquelle et pour l'usage de laquelle la Banque a émis une Carte.
- Comptes liés : tous les comptes à vue, les comptes d'épargne et les dépôts-titres tenus auprès de la Banque et dont l'Abonné est titulaire, cotitulaire, mandataire ou représentant légal.
- Service : le Service PCbanking
- Moyens d'accès et de signature : moyens mis à disposition par la Banque ou acceptés par la Banque et par lesquels l'Abonné peut s'identifier électroniquement et/ou signer des ordres dans le cadre du Service.
- Carte : une carte de débit ou AccessCard émise par bpost banque et liée à l'abonnement.
- Code secret : code chiffré personnel et confidentiel de la Carte servant d'identifiant.
- Lecteur de carte : petit appareil électronique permettant, au moyen d'une signature électronique, de s'identifier de manière sécurisée et de signer des opérations dans le cadre du Service.
- Numéro d'abonnement : numéro attribué par la Banque à l'Abonné et qui permet de l'identifier.
- Compte de référence : compte à vue lié à l'abonnement PCbanking, désigné comme tel par l'Abonné au moment de l'octroi du Service et sur lequel sont comptabilisés les frais éventuels relatifs au Service.
- MOBILEbanking : le service de banque mobile sur tablette ou Smartphone de la Banque.
- Application itsme : l'application mobile offerte par Belgian Mobile ID SA (siège social Place Sainte Gudule 5, 1000 Bruxelles).

Selon les possibilités offertes par la Banque, les fonctionnalités de l'Application itsme peuvent être utilisées comme Moyen d'accès et de signature dans le Service.

- Compte itsme : le compte personnel qui doit être préalablement créé auprès de Belgian Mobile ID SA pour utiliser l'Application itsme.
- Code itsme : code d'identification personnel et confidentiel, créé directement dans l'Application itsme par l'utilisateur pour utiliser l'Application itsme.
- Données de sécurisation personnelles : les moyens personnalisés que la Banque ou une autre banque met à la disposition des utilisateurs afin de s'authentifier. Chaque banque peut employer des moyens différents à cet effet.
- Autre banque : les institutions financières, autres que bpost banque, qui proposent et gèrent des comptes de paiement.

Article 3. Octroi du Service

Le Service peut être octroyé à toute personne physique qui le demande en tant que titulaire, co-titulaire ou mandataire d'au moins un compte à vue sur lequel il a le pouvoir d'agir seul et sans limitation de pouvoirs.

La Banque ne peut pas être contrainte de satisfaire à une demande d'abonnement au Service ni de communiquer les motifs d'une éventuelle décision négative.

Pour utiliser le Service, l'Abonné doit pouvoir disposer d'un accès à internet via un ordinateur qui lui permet de se connecter aux sites internet de la Banque. La Banque publie sur son site internet les exigences techniques (navigateur internet et système d'exploitation) auxquelles l'ordinateur doit satisfaire. Cette page internet est régulièrement mise à jour en fonction de l'évolution technologique. Il est recommandé que l'Abonné consulte cette page régulièrement.

Article 4. Accès aux Comptes liés

Tous les comptes à vue, les comptes d'épargne et les dépôts-titres tenus auprès de la Banque et pour lesquels l'Abonné est titulaire, co-titulaire, mandataire ou représentant légal sont, dès l'octroi du Service, des Comptes liés.

Cependant, les services accessibles à l'Abonné via le Service, concernant les Comptes liés pour lesquels il ne dispose pas du pouvoir d'agir seul et sans limitation de pouvoirs, sont limités à la consultation de l'état de ces comptes et de l'historique des mouvements sur ces comptes.

En tout état de cause, l'Abonné ne peut effectuer que des opérations compatibles avec les pouvoirs dont il dispose sur les Comptes liés.

Article 5. Description des services

5.1. Le Service permet à l'Abonné d'entrer en liaison avec le site PCbanking de la Banque par l'intermédiaire d'un PC pour :

- la consultation de l'état des Comptes liés (solde et historique des mouvements);
- La consultation des produits et services bancaires et d'assurance dont l'Abonné est titulaire;
- la consultation et l'impression des extraits de compte relatifs aux Comptes liés;
- des opérations sur les Comptes liés;
- la demande ou l'achat de produits ou services déterminés offerts par la Banque;
- la gestion de données (ex. liste des bénéficiaires);
- l'échange de messages avec la Banque.

Un aperçu détaillé est aussi disponible sur le site www.bpostbanque.be. La Banque peut toujours ajouter, modifier ou supprimer des fonctionnalités.

Pour les Abonnés mineurs, certains services ne sont pas accessibles, ou de manière limitée seulement.

5.2. Plafonds

Les virements effectués via le Service sont limités, par abonnement, à un montant maximum de 25.000 EUR par jour et de 50.000 EUR par semaine. La limite par transaction est fixée à 25.000 EUR. Ces limites ne sont pas d'application pour les transferts entre comptes liés.

Pour un Abonné mineur, les limites décrites dans les Conditions Générales du Compte Jeunes sont d'application.

La Banque se réserve toutefois le droit de limiter ces montants maximaux à concurrence d'un montant qu'elle fixera elle-même en cas de risque d'escroquerie ou d'abus similaires.

Une opération ne sera effectivement exécutée que si le Compte lié sur lequel elle s'effectue présente une provision suffisante compte tenu des opérations non encore comptabilisées.

5.3. Communication

Dans les limites autorisées par la loi et sans préjudice d'accords dérogatoires avec l'Abonné, un certain nombre d'informations, messages ou documents légaux, réglementaires ou contractuels seront communiqués aux titulaires d'un abonnement PCbanking et/ou MOBILEbanking exclusivement via ces deux canaux digitaux. L'Abonné s'engage à prendre régulièrement connaissance des informations, messages et documents communiqués.

Article 6. Service d'information sur les comptes et service d'initiation de paiement

6.1 Le Service PCbanking offre à l'Abonné la possibilité de recourir aux services de paiement suivants :

- service d'information sur les comptes ;
- service d'initiation de paiement.

L'utilisation de ces services est toujours subordonnée au consentement de l'Abonné, tel que décrit ci-après. Dès que la connexion est établie avec une autre banque, la Banque s'identifiera et communiquera de manière sécurisée.

Les informations relatives au traitement des données à caractère personnel assuré dans ce cadre se trouvent dans la Déclaration Vie Privée de la Banque.

6.2 Service d'information sur les comptes

L'Abonné peut ajouter, à son relevé de compte dans son PCbanking, un ou plusieurs comptes de paiement (généralement de type compte à vue), ouverts auprès d'une autre banque et dont il est (co-)titulaire ou mandataire, et y consulter les informations y afférentes. Les comptes concernés doivent pouvoir être consultables en ligne auprès de l'autre banque. La possibilité d'ajouter ou non des comptes est toujours soumise aux règles et conditions en vigueur auprès de l'autre banque.

L'Abonné peut consulter le solde des comptes ajoutés et l'historique des opérations exécutées.

L'Abonné souhaitant recourir à ce service doit donner son consentement à la Banque quant à l'obtention des données disponibles de ce(s) compte(s) ouvert(s) auprès de l'autre banque. Dans ce cas, il donne son consentement via le Service PCbanking.

L'Abonné a toujours la possibilité de retirer son consentement en supprimant les comptes ajoutés de son relevé de compte dans l'application.

Après recueil du consentement, la Banque établit la connexion avec l'autre banque et l'Abonné doit s'authentifier auprès de celle-ci à l'aide des données de sécurisation personnelles obtenues de cette autre banque. L'autre banque décide de la durée de validité de l'accès sans nécessiter de nouvelle authentification. Cette durée peut varier d'une banque à l'autre, la durée maximale étant fixée à 90 jours. Au terme de ce délai, l'Abonné devra à nouveau se connecter et s'authentifier, faute de quoi ses données ne seront plus mises à jour.

6.3 Service d'initiation de paiement

L'Abonné peut initier un ordre de paiement sur les comptes à vue qu'il détient auprès d'une autre banque, pour autant qu'il les ait ajoutés à son relevé de compte dans son PCbanking.

Dès qu'un Abonné souhaite initier un paiement depuis un compte détenu auprès d'une autre banque, il devra y donner son consentement explicite à la Banque.

L'Abonné indique toutes les données nécessaires à l'initiation du paiement sur l'écran prévu à cet effet, avant d'autoriser la Banque à établir la connexion avec l'autre banque et à transmettre l'ordre de paiement.

La Banque fait basculer l'Abonné dans l'environnement de banque en ligne de l'autre banque, où il devra s'identifier et s'authentifier à l'aide des données de sécurisation personnelles obtenues de cette autre banque. Ensuite, la Banque transmet toutes les données de l'ordre de paiement à l'autre banque.

L'autre banque exécute l'opération conformément aux conditions d'exécution exposées dans le contrat-cadre conclu entre l'Abonné et l'autre banque.

La Banque informe l'Abonné quant à la réussite ou non de l'initiation de l'ordre de paiement sur la base des renseignements fournis par l'autre banque.

6.4. L'Abonné peut avoir accès, par l'intermédiaire d'un prestataire de services tiers, à certaines informations des comptes liés (services d'information sur les comptes) et/ou ordres de paiement sur ces comptes transmis à la Banque (services d'initiation de paiement). Le prestataire de services tiers (fournisseur de services d'information sur les comptes ou d'initiation de paiement) établit à cet effet, moyennant le consentement explicite de l'Abonné, une connexion avec l'environnement de banque en ligne de la Banque. L'Abonné devra ensuite se connecter et s'authentifier au moyen des données de sécurité personnelles reçues de la Banque ou acceptées par celle-ci (p. ex. itsme). Lorsqu'un ordre de paiement est donné par l'intermédiaire d'un prestataire de services d'initiation de paiement, la Banque l'exécute selon les conditions définies dans le contrat-cadre entre l'Abonné et la Banque.

Article 7. Utilisation

7.1. Pour s'identifier lors de la connexion au Service, les ordres à exécuter ou les transactions à signer dans le Service, l'Abonné utilise les Moyens d'accès et de signature suivants :

- soit le Lecteur de Carte, la Carte et le Code secret en conformité avec les instructions reprises dans le manuel d'utilisation. Pour l'accès au Service, l'Abonné doit indiquer également son numéro d'abonnement ;
- soit l'Application itsme.

L'Abonné peut activer le service MOBILEbanking sur son smartphone ou sa tablette avec son Numéro d'abonnement, Lecteur de carte, Carte et Code secret. Une description du service MOBILEbanking et ses conditions d'utilisation sont repris dans les Conditions particulières relatives à l'utilisation du service MOBILEbanking.

7.2. Pour faire usage de l'Application itsme, l'Abonné doit avoir au moins 18 ans. L'Abonné doit s'enregistrer préalablement dans l'Application itsme en créant un Compte itsme et en le couplant à un Code itsme conformément aux conditions convenues entre l'Abonné et Belgian Mobile ID. L'Abonné doit ensuite activer son Compte itsme dans le Service PCbanking. Il utilise à cette fin les Moyens d'accès et de signature mis à sa disposition par la Banque.

Le compte itsme se bloque dans le cas où un Code itsme erroné est encodé à trois reprises. Dans un tel cas, l'Abonné doit à nouveau s'enregistrer dans l'application et demander un nouveau Code. L'Abonné dispose toujours de la possibilité de bloquer ou d'effacer son compte itsme via le site web itsme. En cas de désactivation ou de blocage de l'Application itsme, l'Abonné dispose toujours de l'accès au Service et peut signer des ordres ou des transactions par le biais des Moyens d'accès et de signature mis à sa disposition à cette fin par la Banque.

7.3. L'Abonné reconnaît que l'usage des Moyens d'accès et de signature forme sa signature électronique. L'Abonné reconnaît que la signature électronique apposée au Moyen des moyens d'accès et de signature constitue la preuve valable de son identité et de son consentement sur le contenu des ordres et transactions opérées dans le Service.

Article 8. Obligations et Responsabilités de l'Abonné

8.1. L'Abonné doit utiliser le Service conformément aux conditions qui en régissent l'émission et l'utilisation. Il doit notamment

respecter strictement toutes les instructions relatives aux procédures d'accès et d'utilisation ainsi qu'aux normes de sécurité, telles que décrites dans les présentes Conditions et le manuel d'utilisation.

8.2. L'Abonné ne peut révoquer un ordre de transfert donné dans le cadre du Service, sous réserve d'un ordre de paiement devant être exécuté dans le futur. Celui-ci peut être révoqué jusqu'au jour bancaire ouvrable précédant le jour futur convenu.

8.3. L'Abonné doit prendre toutes les mesures raisonnables pour préserver la sécurité de ses Moyens d'accès et de signature, sauvegarder leur caractère confidentiel et personnel et prévenir tout risque d'utilisation non autorisée.

Ainsi, l'Abonné s'engage notamment :

- à ne jamais communiquer à des tiers son Code secret ou son Code itsme ni à les noter, sur quelque support que ce soit, sous une forme aisément reconnaissable;
- à ne jamais communiquer à des tiers ni ne mettre à leur disposition les Moyens d'accès et de signature;
- à ne jamais communiquer à des tiers les codes fournis par la Carte ou le Lecteur de carte (ni par téléphone, ni par email ou toute autre manière).

L'Abonné vérifie toujours si son ordre de paiement est correct avant de le signer.

L'Abonné qui a activé l'Application itsme pour utilisation dans le Service, est tenu de respecter les obligations et mesures de sécurité relatives à l'utilisation du service itsme reprises dans son contrat avec Belgian Mobile ID.

8.4. L'Abonné prend toutes les mesures de précaution nécessaires afin d'éviter toute utilisation abusive de son ordinateur. Il fait en sorte que son ordinateur soit sécurisé. Il veille à ce qu'un tiers ne soit pas en mesure d'avoir le contrôle de son ordinateur.

8.5. L'Abonné notifie à POSTINFO, dès qu'il en a connaissance, toute perte, vol, détournement ou utilisation non autorisée de ses Moyens d'accès et de signature et tout risque d'utilisation non autorisée de ceux-ci, ainsi que toute imputation sur les extraits de compte d'opérations effectuées via le Service sans son accord et non correctement exécutée, ainsi que toute irrégularité constatée sur les extraits de compte.

POSTINFO peut être joint par téléphone au numéro 022/012345 du lundi au vendredi de 8h à 12h30 et de 13h à 18h, et le samedi de 9h à 13h. Si les faits sont constatés hors ces jours et heures d'accessibilité à POSTINFO, l'Abonné effectue sa notification dès que possible.

Etant donné que le système d'identification et de signature électronique dans le cadre de PCbanking implique l'utilisation d'une Carte et d'un code secret, le détenteur informera immédiatement CARD STOP en cas de perte, de vol, de détournement ou d'utilisation non autorisée de cette Carte et/ou de son code secret, ou de risque d'utilisation non autorisée de cette Carte et de son code secret. L'Abonné veille à prendre les mesures qui lui permettent de se mettre en état de constater sans retard de tels faits. CARD STOP est accessible 7 jours sur 7, 24 heures sur 24 au 078/170.170. L'entretien téléphonique est intégralement pris en charge par CARD STOP.

En cas de perte, de vol, de détournement ou d'utilisation non autorisée, l'Abonné doit également faire une déclaration de ces faits auprès des autorités de police dans les 24 heures de leur constatation et faire parvenir la preuve et les références de cette déclaration à la Banque.

L'Abonné qui a activé l'Application itsme doit également prévenir Belgian Mobile ID et bloquer son compte dès qu'il a connaissance de la perte, du vol ou de l'utilisation frauduleuse de son Compte itsme ou de son appareil. Ceci peut s'opérer via le site internet d'itsme ou en contactant l'helpdesk de itsme (+32 2 657 32 13 durant les heures d'ouverture). Plus d'informations peuvent être trouvées sur le site web d'itsme.

8.6 L'Abonné est responsable de toutes les pertes liées à toute opération non autorisée consécutive à l'utilisation de ses Moyens d'accès et de signature perdus, volés ou détournés, dès qu'ils sont en sa possession jusqu'à la notification prévue au point 4 à concurrence toutefois d'un montant de 50 €. Ce plafond prévu de 50 € n'est cependant pas applicable et l'Abonné supporte toutes les pertes si celui-ci a agi frauduleusement, intentionnellement ou avec négligence grave.

La Banque se réserve le droit d'invoquer comme négligence grave, en tenant compte de l'ensemble des circonstances de fait, notamment le non-respect d'une ou plusieurs obligations énoncées aux points 8.1, 8.3, 8.4 et 8.5, et sans préjudice du droit de l'Abonné d'en appeler à l'appréciation du juge conformément à la loi.

Après la notification effectuée conformément aux dispositions du point 4, l'Abonné n'est plus responsable des conséquences financières résultant de l'utilisation de ses Moyens d'accès et de signature perdus, volés ou détournés sauf s'il a agi frauduleusement. Dans le cas où l'Abonné a constaté les faits hors des jours et heures d'accessibilité du Service Help Desk et a effectué la notification de ces faits dès que possible, il n'est pas responsable des conséquences résultant de la perte, du vol, du détournement ou de l'utilisation non autorisée de ses Moyens d'accès et de signature entre le moment où il a constaté les faits et le moment où il a effectué la notification, sauf s'il a agi frauduleusement.

L'Abonné ne supporte aucune perte s'il n'a pas pu constater la perte, le vol ou l'utilisation illicite avant que le paiement ait eu lieu, sauf lorsqu'il a agi frauduleusement ou intentionnellement ou si la perte est due à des actes ou des manquements d'un employé, d'un agent de la Banque ou d'une entité à qui des activités ont été externalisées.

8.7 L'Abonné qui constate des irrégularités ou des opérations non autorisées sur des comptes détenus auprès de l'autre banque et ajoutés au relevé de compte dans son PCbanking doit s'adresser à son autre banque en vue d'obtenir un éventuel remboursement, même si ces opérations ont été initiées via son PCbanking. La Banque n'intervient pas dans ces litiges.

Si l'Abonné constate la perte, le vol ou l'utilisation illicite de ses données de sécurisation personnelles obtenues de l'autre banque afin de s'authentifier, il doit agir conformément aux dispositions du contrat qu'il a conclu avec cette autre banque.

Article 9. Obligations et Responsabilités de la Banque

9.1 Pour le Service, la Banque a mis en place des systèmes conformes à l'état actuel de la technologie et met en œuvre des

moyens raisonnables pour la sauvegarde de leur sécurité. Elle prend les mesures nécessaires pour garantir la confidentialité des modes d'identification personnels des Abonnés.

Si la Banque constate une fraude présumée ou effective concernant l'abonnement d'un Abonné, elle l'en avertira par téléphone ou par tout autre moyen de communication adapté. À cet égard, la Banque ne demandera jamais de communiquer le code secret de la carte de débit ou un code créé avec la carte de débit ou tout autre code secret ou moyen de sécurité personnel.

La Banque avertit également ses clients par l'intermédiaire des communications générales sur son site web ou des messages généraux dans PCbanking ou MOBILEbanking afin d'attirer leur attention sur d'éventuelles fraudes (p. ex. phishing).

9.2 La Banque enregistre les données essentielles de toute opération effectuée dans le cadre du Service, au moment où celle-ci est effectuée. Ces enregistrements sont conservés par la Banque au moins pendant 10 ans à compter de l'exécution des opérations et peuvent être restitués sous forme lisible sur n'importe quel support standard.

Lorsque l'Abonné nie avoir autorisé une opération exécutée dans le cadre du Service ou affirme que l'opération n'a pas été exécutée correctement, la Banque doit apporter la preuve que l'opération a été authentifiée, correctement enregistrée et comptabilisée et n'a pas été affectée par une déficience technique ou autre.

La Banque apporte valablement cette preuve en produisant les enregistrements relatifs aux opérations contestées sans préjudice d'une preuve contraire apportée par l'Abonné.

Lorsque l'Abonné affirme qu'une opération n'a pas été exécutée correctement, la production des enregistrements est une preuve suffisante pour établir que l'opération a été correctement exécutée.

9.3 La Banque met en place les moyens pour assurer au mieux la continuité du Service. Cependant, la Banque se réserve le droit de procéder, sans indemnité, à des interruptions du Service pour autant qu'elles ne se prolongent pas au-delà d'un délai raisonnable, en cas de nécessité, et notamment pour l'entretien ou pour l'installation de nouvelles versions ou mises à jour des systèmes et dispositifs.

9.4 La Banque est responsable, sous réserve de l'exécution par l'Abonné, de toutes les obligations qui sont à sa charge :

- de l'inexécution ou de l'exécution incorrecte d'un ordre transmis correctement par l'Abonné dans le cadre et selon les normes d'utilisation du Service, à partir de dispositifs, terminaux ou au moyen d'équipements agréés par la Banque;
- des ordres effectués sans autorisation de l'Abonné.

Dans les cas où la Banque est responsable, elle doit, selon le cas :

- rembourser sans tarder le montant de l'opération non exécutée ou mal exécutée, et si besoin est, rétablir le compte lié concerné dans la situation qui aurait prévalu si la mauvaise opération n'avait pas eu lieu;
- rembourser immédiatement le montant de l'opération non autorisée, et le cas échéant, rétablir le compte dans l'état où il se serait trouvé si l'opération non autorisée n'avait pas eu lieu, le cas échéant augmenté des intérêts sur ce montant;

- rembourser les autres conséquences financières éventuelles, notamment le montant des frais supportés par l'Abonné pour la détermination du dommage indemnisable comme suite à l'opération non autorisée.

La date de valeur du remboursement d'un montant d'une transaction sur un compte à la suite de l'alinéa précédent ne sera pas ultérieure à la date à laquelle le montant a été initialement débité du compte concerné.

9.5 Si l'Abonné conteste une opération exécutée sur un compte détenu auprès d'une autre banque et initiée dans le service PCbanking, il doit s'adresser à cette autre banque. L'autre banque constitue en effet le seul point de contact pour l'Abonné. La Banque n'intervient pas dans les litiges opposant l'autre banque à l'Abonné. La Banque et l'autre banque sont chacune responsables de la partie des opérations de paiement dont elles ont la maîtrise. Le cas échéant, l'autre banque prendra contact avec la Banque afin de déterminer ensemble leur part de responsabilité respective. Dans ce cadre, la Banque devra apporter la preuve que l'opération en question a été authentifiée et dûment enregistrée, et qu'elle n'a pas été affectée par une déficience technique ou autre des systèmes placés sous son contrôle. La Banque devra démontrer qu'elle a correctement initié l'ordre de paiement auprès de l'autre banque et que celle-ci a effectivement reçu ledit ordre.

Lorsqu'un ordre de paiement a été initié par l'Abonné par l'intermédiaire d'un prestataire de services d'initiation de paiement, la Banque indemnise le client pour la transaction non exécutée ou incorrectement exécutée et, le cas échéant, remettra le compte dans l'état dans lequel il se serait trouvé si la transaction de paiement incorrecte n'avait pas eu lieu et ce, sans préjudice des dispositions de l'article 8. Le cas échéant, la Banque s'adressera au prestataire de services d'initiation de paiement qui devra fournir la preuve nécessaire que l'ordre a été initié et reçu correctement par la Banque.

9.6 La Banque n'assume aucune responsabilité en cas de dommages, directs ou indirects, qui résulteraient du mauvais fonctionnement de l'équipement de l'Abonné ou du Service de télécommunications offert par un tiers, soit en cas d'interruption du Service pour des causes indépendantes de la volonté de la Banque.

Article 10. Propriété intellectuelle

Tous les droits de propriété intellectuelle sur le service PCbanking et sur l'ensemble des informations, documents, publications concernant ce Service sont détenus par la Banque et/ou, le cas échéant, par ses fournisseurs. L'Abonné se voit accorder un droit d'utilisation personnel, non exclusif et non transmissible pour toute la durée du contrat relatif au Service.

L'Abonné s'engage à respecter ces droits et à s'abstenir de toute violation de ceux-ci. Cela implique notamment de ne pas copier, manipuler, compiler ou modifier, diffuser ou mettre à la disposition de tiers de quelque façon que ce soit des logos, marques, logiciels ou tout autre élément du PCbanking sur lesquels sont détenus de droits de propriété intellectuelle.

Article 11. Tarif et frais

La Banque se réserve le droit de tarifier le Service et les opérations effectuées dans le cadre du Service.

Tous les frais relatifs au Service sont précisés dans la Liste des tarifs visés à l'article 21 des Conditions Générales Bancaires et communiqués à l'Abonné conformément aux dispositions de cet article.

Tous les frais relatifs à l'équipement et au matériel informatique, au fonctionnement de ceux-ci, à l'accès Internet, ainsi que tous les coûts des télécommunications liés aux connexions effectuées dans le cadre du Service sont à charge de l'Abonné.

Article 12. Droit de rétractation en cas de contrat à distance

Lorsque le contrat pour le Service est conclu à distance, l'Abonné a le droit de se rétracter, sans pénalité et sans indication de motif, audit contrat. L'Abonné peut exercer ce droit de rétractation pendant un délai de 14 jours calendriers à dater de la conclusion du contrat, par lettre recommandée adressée à Cards, Credits & Contracts, 1100 Bruxelles. L'Abonné qui a fait usage de son droit de rétractation est tenu de restituer dans les meilleurs délais, et au plus tard dans les 30 jours calendriers à compter de la date de l'envoi de la lettre recommandée précitée, le Lecteur de carte dans n'importe quel bureau de bpost.

À l'expiration du délai de rétractation, le contrat est conclu définitivement et il ne peut y être mis fin qu'aux conditions mentionnées dans l'article 11 ci-dessous.

Sans préjudice à l'alinéa 1^{er} du présent article, l'utilisation du Service pendant le délai de rétractation précité, est considérée comme l'autorisation de l'Abonné de commencer le Service.

Article 13. Blocage et cessation du Service

La Banque peut à tout moment et sans avertissement bloquer le Service en cas de motifs justifiés comme lorsque la sécurité du Service est compromise, la présomption d'un usage non autorisé ou abusif. La Banque informe l'Abonné, si possible, avant le blocage ou, au plus tard, immédiatement après. Cette fourniture d'information n'est pas exigée lorsque cet objectif interférerait avec des préoccupations légitimes de sécurité ou serait lié à une loi ou réglementation. Dès lors que les raisons du blocage n'existent plus, le blocage est levé.

L'Abonné ou la Banque peut mettre fin unilatéralement à l'abonnement, à tout moment et sans devoir communiquer de motif. L'Abonné avise la Banque de la cessation au bureau de poste ou par un écrit adressé à POSTINFO (Boulevard Anspach 1, 1100 Bruxelles). Si la Banque décide de mettre fin à l'abonnement, elle en avertit l'Abonné moyennant préavis préalable de deux mois. Pour des motifs le justifiant, la Banque peut mettre fin immédiatement à l'abonnement en avisant l'Abonné.

En cas de cessation du Service, la redevance annuelle est remboursée au *pro rata temporis*, à partir du mois suivant la date de la cessation.

La clôture du Compte de référence met fin automatiquement à l'Abonnement.

Article 14. Modification

La Banque a la faculté de modifier unilatéralement les présentes Conditions à n'importe quel moment. Un avis de modification sera adressé à l'Abonné, le cas échéant, via le Service, au moins deux mois avant la mise en application de la modification. Les modifications sont à disposition de l'Abonné via le Service. A défaut de réaction dans les deux mois, l'Abonné est réputé avoir accepté les modifications.

Article 15. Extraits de compte

Les extraits de compte relatifs aux comptes liés sont mis à la disposition de l'Abonné, électroniquement, via le Service. Les extraits de compte ne sont plus communiqués par la poste, ni aux titulaires des comptes, ni à l'Abonné, à moins que le titulaire de ce compte l'ait demandé expressément.

Nonobstant les dispositions de l'article 8.4 de ces Conditions particulières, toute contestation relative à une opération non autorisée ou mal exécutée dans le cadre du Service, doit être signalée par écrit, à POSTINFO (Boulevard Anspach 1, 1100 Bruxelles), immédiatement après avoir été constatée sur les extraits de compte et au plus tard dans les 13 mois suivant la date de débit ou de crédit de l'opération contestée. A défaut de protester dans ce délai, l'opération sera réputée être correctement exécutée et approuvée.

Article 16. Plaintes et litiges

Les réclamations en relation avec la Carte ou des services qui y sont liés peuvent être introduites :

- via le formulaire de contact en ligne sur www.bpostbanque.be
- par courrier adressé à Postinfo – bpost banque, Boulevard Anspach 1 à 1000 Bruxelles
- par e-mail adressé à plaintes.bpostbanque@bpost.be
- par téléphone au numéro 022/012345

Si le client n'est pas d'accord avec la solution proposée, il peut également s'adresser au service Customer Services de bpost banque, rue du Marquis 1 boîte 2 à 1000 Bruxelles, ou par email : quality@bpostbank.be.

Après avoir épuisé toutes les possibilités offertes au sein de la Banque, le Titulaire de la Carte ou du compte peut demander l'intervention de l'Ombudsfin – Service de médiation des services financiers par courrier adressée à North Gate II, boulevard du Roi Albert II, n° 8, boîte 2 à 1000 Bruxelles ou par email : Ombudsman@ombudsfin.be ou via 02/545 77 70 ou via le formulaire de contact en ligne sur leur site internet www.ombudsfin.be.

Des réclamations peuvent également être soumises au SPF Économie, PME, Direction générale de l'inspection économique, par courrier adressé à North Gate II, Boulevard du Roi Albert II 16, 1000 Bruxelles par téléphone au 02/277.54.84, par email à eco.inspec.fo@economie.fgov.be ou via le formulaire de contact en ligne sur leur site internet www.economie.fgov.be.