RÈGLEMENT AXA MOBILE BANKING SERVICE
Annexe 1 au Règlement homebanking

Cette annexe au Règlement homebanking régit les droits et obligations du client et de la Banque en ce qui concerne l'accès à et l'utilisation du service mobile banking d'AXA (ci-après «mobile banking»).
Les présentes dispositions font partie intégrante des annexes au Règlement général des opérations d'AXA Bank Europe, ci-après dénommée «la Banque». Les dispositions du Règlement général des opérations et de ses annexes pertinentes sont dès lors d'application, sauf lorsqu'il y est dérogé dans le règlement ci-après.

Sous réserve de l'application d'autres lois et arrêtés, les opérations de paiement via mobile banking sont régies par les dispositions de la loi du 10 décembre 2009 relative aux services de paiement. Dans le présent règlement, il n'est pas dérogé aux dispositions impératives de cette loi. Les dispositions de cette loi reprises dans le présent règlement doivent dès lors être lues et interprétées comme telles.

Article 1: Définitions

- la Banque: AXA Bank Europe SA, dont le siège social est sis en Belgique, Boulevard du Souverain 25, 1170 Bruxelles et titulaire du n° BCE/TVA BE 0404 476 835 RPM Bruxelles;

- le client: toute personne qui, selon le cas a activé ou souhaite activer l'application mobile banking.

- États membres de l'UE: les États membres de l'Union européenne, à savoir la Belgique, la Bulgarie, Chypre, le Danemark, l'Allemagne, l'Estonie, la Finlande, la France, la Guyane française, Gibraltar, la Grèce, la Guadeloupe, la Hongrie, l'Irlande, l'Italie, la Lettonie, la Lituanie, le Luxembourg, Malte, la Martinique, les Pays-Bas, l'Autriche, la Pologne, le Portugal (y compris les Açores et Madère), la Réunion, la Roumanie, la Slovénie, la Slovaquie, l'Espagne (y compris les îles Canaries, Ceuta et Melilla), la République tchèque, le Royaume-Uni, la Suède et [la Croatie] [modifié le 24 juin 2013].

- États membres de l'EEE: les États membres de l'Espace économique européen, à savoir les États membres de l'UE + l'Islande, le Liechtenstein et la Norvège.

- Zone SEPA: les États membres de l'espace unique de paiement en euros («Single European Payments Area»), à savoir les États membres de l'EEE + la Suisse et Monaco.

- Zone euro: les pays qui ont l'euro pour monnaie, à savoir la Belgique, Chypre, l'Allemagne, la Finlande, la France, la Guyane française, la Grèce, la Guadeloupe, l'Irlande, l'Italie, le Luxembourg, Malte, la Martinique, les Pays-Bas, l'Autriche, le Portugal (y compris les Açores et Madère), la Réunion, la Slovaquie, la Slovénie, l'Espagne (y compris les îles Canaries, Ceuta en Melilla), [Estland] [modifié le 24 juin 2013].

- homebanking: une fonctionnalité de la carte bancaire AXA que le client peut activer et qui consiste en un ensemble de procédures lui permettant de gérer à distance ses affaires bancaires via un PC ou autre instrument; son utilisation est régie par le Règlement homebanking; le client a pris connaissance au préalable de ce règlement et en a accepté le contenu.

- appareil: l'instrument donnant accès au mobile banking, à savoir un smartphone, une tablette ou un instrument de même nature; les exigences techniques auxquelles cet appareil doit satisfaire figurent sur le site web de la Banque, www.axa.be (FAQ);

- nom d'utilisateur: un nom personnel avec lequel le client peut s'identifier pour avoir accès au mobile banking à condition que le code secret exact soit utilisé lors de la connexion; le client peut modifier ce nom d'utilisateur à tout moment.

- code secret: un code strictement personnel et confidentiel qui se compose de 6 chiffres et avec lequel le client peut s'identifier pour avoir accès au mobile banking et/ou pour signer des opérations, à condition que le nom d'utilisateur exact soit utilisé lors de la connexion; le client peut modifier ce code secret à tout moment.

- opération (de paiement): une opération initiée par le client via le mobile banking dans le but de transférer de l'argent, quelle que soit par ailleurs la relation entre client et bénéficiaire.

- ordre de paiement: un ordre donné à la Banque par le client d'effectuer une opération de paiement au moyen du mobile banking.

- identifiant unique: le numéro de compte au format IBAN (International Bank Account Number) accompagné du BIC (Business Identifier Code) ou, aussi longtemps qu'il subsiste, le numéro de compte au format BBAN (Belgian Bank Account Number, constitué de 12 chiffres), à communiquer par le client pour identifier le(s) compte(s) sans équivoque lors d'une opération de paiement.

- jour bancaire ouvrable: jour durant lequel les sièges centraux des banques sont ouverts en Belgique. Les samedis, dimanches, jours fériés et jours de fermeture bancaire définis par le secteur bancaire belge ne sont jamais des jours bancaires ouvrables, quels que soient par ailleurs les jours et les horaires d'ouverture des agences locales.

- liste des tarifs: liste détaillée élaborée par la Banque en plusieurs parties, de tous les frais, tarifs, cours de change et autres renseignements relatifs aux différents services proposés par la Banque, parmi lesquels mobile banking. Elle est disponible dans chaque agence et peut également être consultée et imprimée à partir du site web de la Banque (www.axa.be). La liste des tarifs fait partie intégrante du Règlement général des opérations et de ses annexes (règlements particuliers).

- agence: agence bancaire AXA où un agent bancaire indépendant exerce son activité d'intermédiation en services

bancaires et en services d'investissement (au sens de la loi du 22 mars 2006) au nom et pour le compte de la Banque.

Article 2: Description de la fonctionnalité mobile banking

Le mobile banking est une application de la Banque pour les opérations bancaires mobiles.
Grâce au mobile banking, le client peut, via un ou plusieurs appareils conformes, effectuer des opérations bancaires auprès de la Banque et ce, 24 heures par jour et 7 jours par semaine (sauf du samedi soir 22h jusqu'au dimanche matin 6h).

Article 3: Accès, identification et sécurisation

3.1. Pour pouvoir accéder au mobile banking, le client, qui satisfait aux conditions stipulées par la Banque, doit avoir déjà activé la fonctionnalité homebanking, comme spécifié dans le Règlement homebanking.
C'est seulement alors qu'il peut activer la fonctionnalité mobile banking sur tout appareil conforme.

3.2. Pour activer le mobile banking sur un appareil conforme, le client doit d'abord installer l'application nécessaire sur cet appareil.
Il doit ensuite s'enregistrer une fois dans l'application mobile banking de l'appareil.
Le client doit disposer à cet effet des moyens d'accès suivants:
- un lecteur de carte (certifié EPCI),
- une carte bancaire AXA établie à son nom, qui répond aux exigences techniques requises,
- le code secret attribué à la carte bancaire AXA.

Pendant ce processus d'enregistrement, le client doit choisir son nom d'utilisateur et son code secret (composé de 6 caractères) qui constitueront ses moyens d'accès et de signature lors de l'utilisation du mobile banking.

Lorsque le client, au moment de se connecter au mobile banking, utilise 5 fois de suite un code secret erroné, la Banque bloque l'accès au mobile banking. Le client peut faire débloquer l'accès via le call center de la Banque s'il connaît encore son code secret. S'il a oublié son code secret, il doit réactiver le mobile banking moyennant un nouvel enregistrement, comme décrit précédemment.

Toutes les informations nécessaires à cet égard figurent sur le site web de la Banque, www.axa.be (FAQ).

3.3. La sécurité d'utilisation maximale pour le client n'est rendue possible que par l'utilisation discrète et simultanée du nom d'utilisateur et du code secret.

Article 4: Services disponibles en mobile banking

Dès qu'il a accès au mobile banking, celui-ci offre au client les services mentionnés ci-après via son appareil.
L'utilisation effective des différentes fonctionnalités de mobile banking ne peut être limitée qu'en vertu des dispositions du présent règlement.

4.1. Fonctionnalités pour lesquelles le client doit être personnellement connecté

4.1.1. "comptes"

Le client peut, via l'option « comptes », consulter le solde de ses comptes à vue et d'épargne (tenus en euros), dont il est titulaire, cotitulaire (avec procuration), représentant légal ou mandataire. Les comptes soldés et les comptes bloqués n'apparaissent pas.
Pour les mineurs d'âge ou les mandataires qui ne sont pas titulaires ou cotitulaires, cette fonctionnalité peut être limitée, en application ou non des instructions données à la Banque à cet égard.

Lors de la consultation des comptes, il est également possible de demander les données détaillées pour chaque compte, ce qui permet d'obtenir une vue d'ensemble des opérations.

4.1.2. « nouveau virement »

4.1.2.1. Le client peut, via l'option «nouveaux virements», introduire des ordres de virement en euros, [suivant les limites définies à l'article 6] [modifié le 7 octobre 2013]

4.1.2.2. Tous les ordres de paiement avec un compte à vue ou un compte à vue start2bank en tant que compte donneur d'ordre, leur exécution par la Banque, les délais d'exécution maximums et […] [modifié le 7 octobre 2013] les ordres de virement avec une date d'exécution souhaitée dans le futur sont régis par les règles relatives aux ordres de virement initiés via selfservice au moyen de la carte bancaire AXA, telles qu'elles figurent dans le Règlement carte bancaire AXA.

4.1.2.3. Tous les ordres de paiement avec un compte d'épargne ou un compte d'épargne start2bank en tant que compte donneur d'ordre sont régis par le Règlement comptes d'épargne, respectivement le Règlement compte d'épargne start2bank, étant entendu que, via mobile banking, aucun virement n'est possible d'un compte d'épargne vers un autre compte d'épargne au nom du conjoint ou d'un membre de la famille jusqu'au 2ème degré du (des) titulaire(s); seul un virement vers un autre compte d'épargne ou un compte à vue au nom du même (des mêmes) titulaire(s) que celui (ceux) du compte d'épargne donneur d'ordre est possible.

4.1.2.4. Une date mémo ou date d'exécution dans le futur […] [modifié le 7 octobre 2013] doit se situer dans le futur, avec un maximum d'un an. Le client peut aussi annuler les virements européens enregistrés avec une date d'exécution dans le futur ou modifier cette date. A cet effet, une signature est toujours nécessaire, tel que décrit à l'article 7.

4.1.2.5. Les virements introduits via mobile banking pour lesquels plus d'une signature est requise seront refusés.

4.1.2.6. S'il existe des montants plafonds pour certains comptes, un virement qui dépasse ce plafond sera refusé (voir également l'article 6).

4.1.2.7. Les mineurs d'âge (12-17 ans) n'ont pas la possibilité d'effectuer de virements depuis un

compte d'épargne.
Pour les personnes majeures, cette possibilité est limitée conformément aux conditions et modalités des comptes d'épargne.

4.1.2.8. Chaque ordre de virement doit être signé et transmis séparément à la Banque. Le client reconnaît la validité légale des ordres de virement donnés par lui, comme décrit à l'article 7.2.

4.1.2.9. Le client peut, après l'avoir complété, envoyer l'ordre de virement par mail afin de pouvoir livrer la preuve de l'ordre de virement. Ce mail ou une copie de celui-ci ne constitue pourtant pas une preuve de l'exécution effective de l'ordre. Cela dépend du solde disponible sur le compte au moment où le virement doit être exécuté.

4.1.3. « cartes de crédit »

4.1.3.1. Le client peut, via l'option « cartes de crédit », consulter un relevé de la (des) carte(s) de crédit portant le logo VISA, dont il est personnellement le titulaire. Par contre, la (les) carte(s) de crédit AXA portant le logo Mastercard ne sont pas visualisées.

4.1.3.2. Par carte, il pourra également consulter un relevé des opérations de paiement qu'il a effectuées avec cette carte au cours des 90 derniers jours. Les opérations enregistrées mais non encore facturées seront visibles sous les « dépenses courantes », tandis que les opérations déjà facturées seront visibles sous les « dépenses payées ».

4.1.3.3. Partant de la limite de dépenses, attribuée au titulaire et liée à la carte, le solde encore disponible sera visualisé pour la période de facturation en cours.
Ce montant peut éventuellement différer du montant réellement disponible parce que des transactions effectuées qui n'ont pas encore été comptabilisées peuvent encore manquer sur le relevé. Pour plus d'informations le client peut contacter Atos Worldline au n° 02/205.85.85.

4.1.3.4. Toutes les informations que le client/titulaire de carte peut consulter via cette option sont mises à disposition par des tiers, comme stipulé à l'article 5, qui est donc invariablement d'application.

4.1.4. « votre agent bancaire AXA »

Le client peut, via l'option «votre agent bancaire AXA », consulter les coordonnées de son (ses) agent(s) bancaire(s) AXA.

4.1.5. « préférences »

Le client peut, via l'option « Modifier les paramètres », modifier son nom d'utilisateur, son code secret et le choix de la langue.

4.2. Fonctionnalités pour lesquelles le client ne doit pas être personnellement connecté

4.2.1. « agents bancaires AXA »

Le client peut, via l'option « agents bancaires AXA », rechercher les coordonnées d'un agent bancaire AXA. Sur la base d'un code postal ou du nom d'une commune, une liste d'agents bancaires AXA lui sera proposée.

4.2.2. « self-service AXA »

Le client peut, via l'option « self-service AXA », rechercher le lieu où il peut trouver un guichet automatique bancaire. Sur la base d'un code postal ou du nom d'une commune, une liste d'agences bancaires AXA équipées d'un appareil self-service lui sera proposée.

4.2.3. « aide »

Le client reçoit, via l'option « aide », des informations sur:
- les coordonnées et l'accessibilité du call center de la Banque,
- la FAQ concernant mobile banking,
- une démo présentant le fonctionnement de mobile banking.

4.2.4. « Card Stop »

Via l'option « card stop », le client peut retrouver toutes les informations concernant ce qu'il doit faire s'il a perdu ses cartes ou l'une de ses cartes, ou lorsqu'elles ont été volées ou avalées par un guichet automatique (bancaire) et prendre directement contact avec Card Stop comme il est précisé dans les Règlements carte bancaire, carte proton, cartes de crédit et maxi prepaid AXA.

4.2.5. « conditions »

Via cette option, le client peut consulter le présent Règlement AXA mobile banking service.

Article 5: Informations provenant de tiers

Lorsque le client demande ou consulte via mobile banking, pour quelque raison que ce soit, des informations mises à disposition par des tiers, la Banque ne peut être tenue responsable du caractère inexact, incomplet ou imprécis de ces informations. Provenant d'une source externe, elles ne peuvent davantage faire naître une quelconque obligation dans le chef de la Banque.

Mobile banking peut contenir des hyperliens vers le site web de tiers. Le client est libre de visiter ou non ces sites web. La Banque n'est nullement responsable du contenu de ces sites ou de leur niveau de sécurisation. Elle ne peut pas davantage être tenue responsable de tout dommage ou de toute conséquence négative qui résulterait pour le client de l'utilisation de données fournies par l'intermédiaire de ces liens ou de la consultation de sites web auxquels ces derniers réfèrent.

Article 6: Limites

Pour des raisons de sécurité, les limites suivantes sont appliquées aux opérations de paiement via mobile banking:

Pour des ordres de virement vers des bénficiaires qui dans homebanking sont repris dans « la liste des bénéfciaiciares » :

* Le montant total de tous les ordres de virement est limité à 2500 EUR par jour (0-24h) et par client.

* Pour les mineurs d'âge (12-17 ans), la limite journalière est fixée à 250 EUR. Ces limites ne peuvent être augmentées, même avec l'accord exprès du représentant légal

[Pour les ordres de virement vers des bénéficiaires qui dans homebanking ne sont pas repris dans « la liste des bénéficiaires » :

* Le montant total de tous les ordres de virement est limité à 500 EUR par jour (0-24h) et par client.

* Pour les mineurs d'âge (12-17 ans), la limite journalière est fixée à 50 EUR. Ces limites ne peuvent être augmentées, même avec l'accord exprès du représentant légal.][modifié le 7 octobre 2013]

Dès qu'un ordre de paiement dépasse l'une de ces limites, l'ordre n'est pas exécuté.

Article 7: Imputation des opérations et preuve.

7.1. Connexion à mobile banking

L'utilisation simultanée de l'appareil sur lequel mobile banking est activé ainsi que du nom d'utilisateur et du code secret que le client a lui-même créés afin de lancer une session mobile banking selon les instructions du système, constitue la preuve de l'identité du client.

7.2. Imputation des opérations de paiement

Toute opération de paiement qui est ensuite -entre le démarrage d'une session effectué de cette façon et sa clôture- introduite et confirmée avec le code secret du client, est réputée avoir été exécutée avec l'autorisation du client et reconnue comme légalement valable par le client.
L'un et l'autre constituent, pour l'application du présent règlement, la signature du client. Les ordres de paiement qui sont correctement introduits par le client sont donc enregistrés par la Banque et seront exécutés si les avoirs disponibles sur les comptes concernés le permettent et pour autant que l'ordre de paiement soit conforme aux conditions et modalités qui s'appliquent à ces comptes.
Un ordre de paiement écrit identique à un ordre de paiement introduit via mobile banking sera toujours traité comme un nouvel ordre de paiement.

7.3. Preuve des opérations de paiement

Toutes les données de chaque opération de paiement introduite et/ou exécutée au moyen de mobile banking sont enregistrées au moment de l'opération et conservées par la Banque pendant au moins cinq ans, afin de pouvoir les reproduire par la suite sous une forme lisible sur un support.
La Banque est toujours présumée responsable du traitement de ces données.
L'impression éventuelle par le client à la suite d'une opération avec mobile banking n'a qu'une valeur informative et ne porte en rien préjudice à la force probante des enregistrements de la Banque.
En cas de litige avec le client concernant une opération, la Banque fournit pour sa part la preuve de cette opération au moyen de ces données, nonobstant le droit du client d'apporter la preuve contraire.

Article 8: Droits et obligations afférents au mobile banking

Sans préjudice des droits et obligations afférents à la carte bancaire AXA et au homebanking et reposant sur la Banque et sur le client, les droits et obligations suivants s'appliquent spécifiquement à l'utilisation de mobile banking.

8.1. Droits et obligations de la Banque

1°-Par le biais du canal choisi par le client pour la réception de ses extraits de compte, la Banque informe le client de toutes les opérations de paiement réalisées au moyen de mobile banking.
Pour chaque opération, l'information contient une description par le biais de laquelle le client peut vérifier l'opération visée.
Pour les opérations de paiement sur compte à vue et compte d'épargne, elle comporte éventuellement le nom et l'identifiant unique du bénéficiaire, le montant de l'opération exprimé en euros et enfin, la date valeur de l'inscription au débit ou au crédit ou la date et le moment de l'opération.
Pour les extraits de compte, les dispositions reprises dans le Règlement comptes à vue, le Règlement compte à vue start2bank, le Règlement comptes d'épargne et le Règlement compte d'épargne start2bank sont applicables.

2°-La Banque empêchera toute nouvelle utilisation de mobile banking dès l'instant où la notification de la perte, du vol ou de l'abus dont question ci-après a eu lieu. Elle peut également empêcher tout nouvel usage dès l'instant où elle a été avertie d'une erreur, d'une irrégularité ou d'une imputation indue.

3°-La Banque garantit le maintien de la confidentialité des moyens d'accès au mobile banking au sein de sa propre organisation et de son propre réseau. Tant la Banque que le client courent des risques graves, en particulier d'abus et d'accès indésirable au mobile banking, si cette confidentialité n'est pas recherchée et contrôlée par toutes les parties concernées.

4°-La Banque se réserve le droit de refuser d'exécuter certaines opérations de paiement via mobile banking, comme le prévoit le Règlement carte bancaire AXA, chaque fois qu'elle le juge utile pour la sécurité du système ou la défense de ses intérêts financiers ou ceux du client.

5°-Outre le droit dont elle dispose de bloquer la carte bancaire AXA comme prévu dans le Règlement carte bancaire AXA, et de bloquer le homebanking comme prévu dans le Règlement homebanking, la Banque se réserve le droit de bloquer l'accès au mobile banking chaque fois qu'elle le juge utile pour la sécurité du système ou pour ses intérêts financiers ou ceux du client, et ce notamment dans les cas suivants:
- lorsqu'un code secret erroné a été encodé plusieurs fois de suite;
- lorsqu'il y a eu opposition à l'usage de mobile banking par le client;
- lorsque le droit d'utilisation de mobile banking prend fin, pour quelque raison que ce soit;
- lorsque les instructions de sécurité et les conditions d'utilisation sont manifestement foulées aux pieds;
- lorsque la Banque constate que l'application mobile banking reste ouverte et inutilisée pendant un laps de temps inutilement long chez le client.

6°- La Banque se réserve le droit de refuser l'accès au service mobile banking.

7°- La Banque garantit autant qu'elle le peut la continuité de mobile banking et des services qui y sont liés. La Banque peut interrompre temporairement le service mobile banking pour des raisons d'entretien, d'amélioration ou de sécurisation, ou pour l'installation de nouvelles versions du logiciel; dans de telles circonstances, elle mettra tout en œuvre pour limiter ces

interruptions à un minimum; les interruptions ne donnent au client aucun droit à une indemnité.

8°- La Banque se réserve le droit de limiter les opérations de paiement à un montant fixé par elle, lorsqu'elle constate qu'il existe un risque d'abus.

8.2. Droits et obligations du client

1°-Le droit d'accès à et l'utilisation de l'application mobile banking, tout comme la carte bancaire AXA et le homebanking, sont personnels et non transférables. Le client ne peut donner accès à aucun tiers à son application mobile banking (pas même à une connaissance, un mandataire, un conjoint ou un membre de la famille). Plusieurs clients peuvent activer mobile banking sur un même appareil. Ils doivent toutefois utiliser chacun l'application avec leurs moyens d'accès et de signature personnels.

2°-Le client a l'obligation de prendre toutes les mesures de précaution raisonnables pour assurer la sécurité du mobile banking ainsi que la confidentialité des moyens d'accès et de signature. Le client doit à son tour respecter rigoureusement la confidentialité de ces moyens d'accès et de signature. Tant la Banque que le client courent des risques graves, en particulier d'abus et d'accès indésirable au mobile banking si cette confidentialité n'est pas recherchée et contrôlée par toutes les parties concernées.

3°-Outre les mesures préventives que tout titulaire d'une carte bancaire AXA doit prendre concernant la sécurité de celle-ci et la confidentialité du code secret et qui sont décrites dans le Règlement carte bancaire AXA, et sans préjudice des mesures de précaution que le client doit prendre en vue d'assurer la sécurité du homebanking, comme stipulé dans le Règlement homebanking, le client prendra, pour la fonctionnalité mobile banking, les mesures de précaution complémentaires suivantes:
- il ne communiquera jamais ni ne mettra à la disposition d'un tiers ses moyens d'accès et de signature à mobile banking (même s'il s'agit d'une connaissance, d'un mandataire, de son conjoint ou d'un membre de sa famille); le client est toutefois autorisé, si nécessaire, à mandater un tiers habilité à accéder aux comptes pour lesquels il le souhaite et qui sont consultables sur mobile banking, auquel cas cette personne pourra avoir accès personnellement à mobile banking pour le compte du client, mais via ses propres moyens d'accès et de signature;
- il ne conservera jamais son code secret pour mobile banking sur son appareil, un PC ou un autre support, n'en fera pas une programmation fixe ni ne le notera de manière identifiable dans un agenda ou un carnet de notes, sur un écrit qu'il porte sur lui ou sur des documents ou pièces rangées dans un endroit non protégé;
- il ne donnera jamais à un tiers accès à son appareil qu'après avoir entièrement achevé la session mobile banking; il ne mettra dès lors jamais son appareil à la disposition de tiers qu'après s'être assuré que l'application mobile banking n'est pas accessible à un tiers quelconque;
- le client fera intervenir le fournisseur de son appareil, s'informera sur les possibilités de protection de son appareil et avertira la Banque lorsqu'il reçoit des signaux indiquant qu'un tiers peut accéder, accède ou tente d'accéder abusivement à son appareil, au service mobile banking et/ou à toutes les connexions de télécommunication et autres avec son appareil;
- pendant une session mobile banking ouverte, il ne quittera pas son appareil, pour quelque raison que ce soit, même pour un très court laps de temps;
- il clôturera toujours immédiatement l'application mobile banking sur son appareil après usage;
- aux divers stades de confirmation d'une opération de paiement, il vérifiera systématiquement si le numéro de compte du bénéficiaire correspond effectivement au numéro de compte souhaité;
- en cas de perte ou de vol d'un appareil sur lequel il a activé mobile banking, le client bloquera ou fera bloquer immédiatement l'application mobile sur cet appareil, conformément aux dispositions de l'article 9.1 ci-après.
[- il respectera les systèmes de sécurité incorporés dans son appareil, lui permettant d'utiliser mobile banking en toute sécurité ; il ne coupera jamais lui-même ces systèmes de sécurité.] [modifié le 7 octobre 2013].

Sous réserve de l'appréciation d'un juge qui tiendra compte de l'intégralité des circonstances matérielles, les mesures de précaution énumérées ici, accompagnées des mesures de précaution auxquelles tout titulaire d'une carte bancaire AXA et tout utilisateur de homebanking doit rester attentif, sont à ce point importantes et à ce point évidentes que leur non-respect peut être considéré comme une négligence grave dans le chef du client, ce qui aura pour effet que la limitation de la responsabilité du client dont question ci-dessous ne sera pas d'application.

4°-Le client est tenu de respecter rigoureusement les conditions et modalités d'utilisation fixées dans le présent règlement.

5°-Le client s'engage à n'effectuer via mobile banking aucune opération de paiement susceptible d'entraîner le dépassement des fonds disponibles à ce moment sur le compte concerné. Le client autorise sans aucune réserve la Banque à débiter son compte de tous les montants payés à l'aide de mobile banking, même si les fonds disponibles ne sont pas suffisants. Le solde débiteur irrégulier qui pourrait ainsi être crée, ne peut pas être considéré comme un octroi de crédit et doit immédiatement être apuré.

6°-Le client n'est pas autorisé à révoquer un ordre de paiement initié via mobile banking à partir du moment où il a autorisé l'exécution de l'opération de manière convenue, l'ordre étant alors réputé avoir été reçu par la Banque, sans préjudice de ce qui est prévu dans le Règlement comptes à vue et dans le Règlement compte à vue start2bank pour la révocation de virements avec date mémo ou date d'exécution souhaitée dans le futur […] [modifié le 7 octobre 2013].

7°-Lors de la modification de son code secret, il choisit un nouveau code qui n'est pas trop à la portée de tiers – comme, par exemple, une partie de la date de naissance, le code postal de la commune, une partie d'un numéro de téléphone, etc.
La modification d'un code secret en un code qui est également utilisé pour d'autres instruments de paiement et moyens d'accès doit être évitée et augmente le risque d'un éventuel usage abusif.
S'il a des motifs fondés de croire que la confidentialité de son code a été violée, il modifiera immédiatement ce code via son appareil.

Article 9: Perte, vol et usage abusif ou non autorisé par des tiers

9.1. Perte, vol et utilisation abusive ou non autorisée de l'appareil

En cas de perte ou de vol de l'appareil ou en cas de présomption d'usage abusif de l'appareil quel qu'il soit, le client doit immédiatement faire bloquer l'application mobile

banking sur cet appareil.

Il peut procéder à cette fin :
- soit lui-même, en bloquant mobile banking sur son appareil via homebanking,
- soit en prenant contact avec le call center de la Banque au numéro +32 3 286 66 21 et faire bloquer mobile banking via le call center,
Si le client est titulaire d'un compte à vue ou compte d'épargne classique, il peut aussi se rendre chez son agent bancaire AXA pour faire bloquer mobile banking.

Si plusieurs utilisateurs ont activé mobile banking sur l'appareil concerné, chacun d'entre eux doit faire bloquer séparément mobile banking de l'une des trois manières susmentionnées.

Le client peut bien entendu réinstaller ensuite mobile banking sur un (autre) appareil, via l'enregistrement prévue à l'article 3.2.

9.2. Falsification, usage abusif ou non autorisé et perte ou vol du nom d'utilisateur et du code secret

Dès que le client soupçonne ce genre de falsification, vol ou usage abusif de ses moyens d'accès et de signature, sans que son appareil ait été perdu ou volé, il doit immédiatement modifier ses moyens d'accès et de signature via mobile banking.
Si cela s'avère souhaitable ou nécessaire, il peut aussi bien entendu bloquer mobile banking comme stipulé à l'article 9.1.

9.3. Déclaration auprès de la police

Dès que le client constate un usage abusif de mobile banking, que ce soit ou non après une perte ou un vol de son appareil ou de ses moyens d'accès ou de signature, il doit immédiatement en faire la déclaration auprès de la police fédérale et remettre ensuite à la Banque une copie du procès-verbal établi dans ce cadre.
Il doit également informer immédiatement la Banque de cet abus, comme stipulé à l'article 10.

9.4. Conséquences

(1) Jusqu'au moment de la notification susmentionnée, le client reste responsable de toutes les conséquences résultant de la perte ou du vol de l'appareil ou de l'usage abusif de mobile banking. Cette responsabilité, pour le client qui opère en dehors de ses activités d'entreprise ou professionnelles, est toutefois limitée à un montant de 150 euros, SAUF si le client s'est rendu coupable d'une négligence grave ou d'un acte frauduleux, auxquels cas cette limitation de responsabilité n' est pas applicable.

Sans préjudice de ce qui a été souligné précédemment au sujet des mesures élémentaires de prudence visant la protection de mobile banking et des moyens d'accès et de signature, peut être considéré comme négligence grave, sans préjudice de l'appréciation du juge, le fait:
- de noter sous une forme aisément reconnaissable, le code secret, sous quelque forme que ce soit, sur un document conservé avec l'appareil ou le fait de le conserver dans l'appareil, un PC ou un autre support.
- de ne pas notifier immédiatement la perte, le vol ou l'usage abusif de l'appareil ou des moyens d'accès et de signature (une telle déclaration ne souffrant aucun report).
- de donner la possibilité à un tiers, quel qu'il soit, de prendre connaissance du code secret et/ou d'utiliser une application mobile banking activée par le client sur un appareil.
- d'omettre de notifier immédiatement à la Banque tout soupçon ou de toute constatation d'un usage abusif.
- d'omettre de notifier immédiatement à la Banque l'imputation, constatée sur les relevés ou sur les extraits de comptes, de toute opération effectuée avec mobile banking pour laquelle aucune autorisation n'a été donnée ou qui n'aurait pas été exécutée correctement.
- d'omettre la notification immédiate à la banque de toute erreur ou irrégularité constatée sur les relevés ou les extraits de compte.
- d'abandonner l'appareil sur lequel l'application mobile banking est activée, dans un véhicule ou un endroit accessible au public, sauf lorsqu'il se trouve dans un tiroir ou une armoire fermant à clé. Sont considérés comme endroits accessibles au public les endroits auxquels un grand nombre de personnes ont effectivement accès sans qu'il s'agisse nécessairement de lieux publics.
- de refuser de déposer immédiatement plainte auprès des services de police en cas d'usage abusif effectif du mobile banking ou de refuser de remettre immédiatement à la Banque une copie du procès-verbal établi lors du dépôt de la plainte.
- d'utiliser mobile banking à l'encontre des conditions contractuelles concernant l'accès et l'utilisation.
- de ne pas (faire) bloquer mobile banking lorsque la Banque en fait la demande.
- de ne pas (faire) bloquer immédiatement mobile banking lorsque le client reçoit des signaux indiquant qu'un tiers peut accéder, accède ou tente d'accéder abusivement à son appareil, au service mobile banking, à certaines de ses fonctionnalités et/ou à sa (ses) connexion(s) de télécommunication ou Internet.
- de communiquer ou de mettre à disposition d'un tiers, quel qu'il puisse être, des moyens d'accès ou de signature.
- de quitter son appareil, pour quelque raison que ce soit, pendant une session mobile banking ouverte, même pour un très court laps de temps.

(2) Dès qu'il a bloqué ou fait bloquer mobile banking, le client cesse d'être responsable pour les conséquences de la perte, du vol ou de l'usage abusif de son appareil ou de ses moyens d'accès et de signature, SAUF si une négligence grave dans le chef du client est prouvée. C'est notamment le cas s'il devait apparaître qu'en dépit de la notification, le client continue à utiliser lui-même mobile banking et/ou tente d'y accéder.

(3) S'il s'avérait que, postérieurement à une notification, mobile banking a été utilisé sans présentation physique ni identification électronique ou que les moyens d'accès et de signature ont été contrefaits par un tiers ou qu'il a été utilisé indûment alors qu'au moment de la (des) opération(s) contestée(s), le client était en possession de l'appareil sur lequel il a activé l'application mobile banking et les moyens d'accès et de signature, le client n'en supportera pas les conséquences, sauf exceptions admissibles en vertu de la loi. Ainsi, si l'existence d'une fraude devait être établie, le client pourra, même après la notification, en cas d'utilisation sans présentation physique ni identification électronique, être tenu de toutes les conséquences liées à cet usage.

Article 10: Opérations de paiement non autorisées ou non correctement exécutées au moyen de mobile banking

10.1. Sans préjudice des mesures exposées ci-dessus en cas de perte, de vol ou d'usage abusif ou non autorisé de l'appareil ou des moyens d'accès et de signature, le client doit informer **sans retard** la Banque de toute opération de paiement non autorisée ou opération non correctement exécutée via mobile banking, dont il constate l'existence.

Il s'adresse pour ce faire à son agence où un dossier de contestation sera dressé.

Si le client est uniquement titulaire de comptes start2bank, il peut, via homebanking (option «Messages»), notifier à la Banque la (les) opération(s) de paiement non autorisée(s) ou non correctement exécutée(s). Si le client n'a plus de carte(s) qui pourrai(en)t lui donner accès à homebanking pour la notification, il peut s'adresser par écrit au service DOB Customer Relations – code postal interne B11/459, Grotesteenweg 214, 2600 Berchem ou envoyer un mail à start2bank.info@axa.be. Dans les deux cas, la Banque prendra contact avec le client le plus vite possible pour le traitement du dossier concernant les opérations contestées.

10.2. Indépendamment de l'obligation qui repose sur le client d'informer immédiatement la Banque de l'existence de toute opération de paiement non autorisée ou non correctement exécutée saisie via mobile banking dès qu'il la constate, le client perd, 13 mois après la date valeur de l'inscription du montant correspondant au débit ou au crédit, le droit de contester les opérations non autorisées ou non correctement exécutées dûment notifiées par la Banque conformément aux modalités et à la périodicité choisies par lui. À l'expiration de ce délai, l'imputation de l'opération est présumée définitive et ne peut plus faire l'objet d'aucune contestation.

À défaut d'une notification en temps opportun par le client, la Banque ne peut être tenue pour responsable de l'opération de paiement non autorisée ou non correctement exécutée qui est contestée.

Le client qui agit dans le cadre de ses activités d'exploitation ou professionnelles ne dispose que d'un délai de 30 jours, à compter de la date valeur de l'inscription au débit ou au crédit du montant correspondant, pour contester une opération non autorisée ou non correctement effectuée, exécutée via mobile banking.

10.3. Sauf lorsqu'il peut prouver qu'il se trouvait dans l'impossibilité de prendre connaissance des informations mises à sa disposition, par extrait de compte et de la manière choisie par lui, concernant les opérations avec mobile banking, et qu'il n'était donc pas en mesure d'informer la Banque **sans délai**, comme prévu à l'article 10.1., d'une opération de paiement non autorisée ou non correctement exécutée, le client est réputé avoir pris connaissance, dans les 30 jours à compter de la date valeur du débit ou crédit du compte concerné, de l'information mise à sa disposition et informer la Banque des opérations non autorisées ou non correctement exécutées au plus tard 60 jours après la date valeur.
Passé ce délai, la Banque considère que l'information du compte est définitivement approuvée et constitue la preuve des opérations effectuées par mobile banking, sauf preuve contraire.

10.4. Lorsque le client nie avoir autorisé une opération de paiement effectuée via mobile banking, ou affirme qu'une opération de paiement n'a pas été correctement effectuée, il incombe à la Banque de prouver que l'opération de paiement a été authentifiée, correctement enregistrée et dûment exécutée et n'a pas été influencée par un problème technique ou une quelconque autre défectuosité. Lorsque le client agit dans le cadre de ses activités professionnelles ou d'entreprise, il doit fournir la preuve qu'il n'a pas autorisé l'opération ou qu'elle n'a pas été effectuée correctement.

Article 11: Traitement des plaintes et recours extrajudiciaires

Sans préjudice de ce qui a été stipulé à l'article 1.30. du Règlement général des opérations (traitement des plaintes) et à l'article 11 du présent règlement (opérations de paiement non autorisées ou non correctement exécutées, le client dispose des moyens suivants:

Le client dispose du droit d'introduire une action, prévue par la législation sur les pratiques de commerce, en cessation des infractions à la loi du 10 décembre 2009 relative aux services de paiement.

Le client particulier peut s'adresser à l'Ombudsman en conflits financiers, comme prévu à l'article 1.30. du Règlement général des opérations.

Le client peut également s'adresser à la Direction Générale du Contrôle et de la Médiation près du Service public fédéral de l'Économie, des PME, des Classes moyennes et de l'Énergie, NG III, avenue Roi Albert Ii 16 , 3ème étage à 1000 Bruxelles, téléphone: +32 2 277 54 84, fax: +32 2 277 54 52, e-mail: eco.inspec.fo@economie.fgov.be.
Le client peut à cet effet utiliser des formulaires disponibles sur le site web: mineco.fgov.be.

Article 12: Responsabilité

12.1. La Banque ne garantit l'exécution correcte et dans les délais, au sein de son organisation, d'opérations introduites correctement et réglementairement par le client par le biais d'un appareil conforme, qu'à condition que lors de l'utilisation de mobile banking pour les opérations concernées, les conditions et modalités d'utilisation aient été strictement respectées. Elle ne peut en aucun cas être tenue responsable de l'usage de mobile banking au moyen d'autres appareils et/ou à l'encontre des conditions et modalités d'utilisation.

12.2. Lorsque le client est le payeur dans le cadre d'un ordre de paiement initié via mobile banking, par exemple un virement, la Banque est responsable vis-à-vis du client de l'exécution correcte et dans les délais de l'opération de paiement, conformément aux dispositions du présent règlement. La responsabilité de la Banque ne peut être engagée que jusqu'au moment où la banque du bénéficiaire perçoit le montant de l'opération de paiement. La Banque fournit la preuve de ce qui précède.

Lorsqu'une opération de paiement saisie via mobile banking n'est pas exécutée ou n'est pas exécutée comme il se doit, la Banque – quelle que soit sa responsabilité en la matière – tentera immédiatement, pour autant qu'elle en ait la possibilité et que le client le lui demande

expressément, de tracer l'opération de paiement; elle informera le client du résultat de ses recherches.

12.3 Un ordre de paiement, donné par mobile banking, exécuté conformément à l'identifiant unique, est réputé dûment exécuté pour ce qui concerne le bénéficiaire indiqué le bénéficiaire indiqué par cet identifiant unique. Si l'identifiant unique fourni par le client est inexact, la Banque n'est pas responsable, au titre de l'article 12.1. de l'inexécution ou de la mauvaise exécution de l'opération de paiement. La Banque ne doit pas vérifier si l'identifiant unique correspond aux éventuelles informations complémentaires données par le client, entre autres le nom du bénéficiaire. Le client est lui-même responsable de toute erreur en la matière.

Dans ces cas, la Banque s'efforcera néanmoins dans la mesure du raisonnable, à la demande du client, de récupérer les fonds engagés dans l'opération de paiement. Les frais mentionnés à cet effet dans la liste des tarifs sont alors facturés. La Banque fera à cet effet des efforts raisonnables sans toutefois pouvoir garantir le remboursement effectif.

Si le client donne un identifiant unique incomplet ou erroné, tant la Banque que la banque du bénéficiaire peuvent facturer des coûts et/ou refuser l'opération. Les coûts facturés par la Banque, le cas échéant, sont repris dans la liste des tarifs. Les tarifs appliqués par la banque du bénéficiaire diffèrent d'une banque à l'autre et d'un pays à l'autre. En cas de données incomplètes ou incorrectes, les coûts facturés sont répercutés sur le client, même si le paiement est restitué à la Banque sans avoir été exécuté.

12.4. Après examen de la légitimité d'une plainte, la Banque, dont la responsabilité serait engagée pour avoir exécuté une opération de paiement non autorisée ou incorrectement exécutée via mobile banking, procédera à la rectification et à la compensation, dans les plus brefs délais, du montant de l'opération non exécutée ou incorrectement exécutée en appliquant la date valeur correcte; de la somme éventuellement nécessaire pour rétablir le client dans la situation dans laquelle il se trouvait avant l'opération non autorisée, en appliquant la date valeur correcte; des autres conséquences financières éventuelles, notamment le montant des frais supportés par le client pour déterminer le dommage indemnisable, pour autant que le client puisse prouver lesdites conséquences, les frais y afférents et le lien de causalité avec l'opération incriminée; de la perte financière résultant de l'exécution incorrecte des opérations lorsque cette exécution est due au dysfonctionnement de l'application mobile banking agréée par la Banque.

Cette disposition s'applique exclusivement si le client agit en dehors de ses activités professionnelles ou d'entreprise. Si le client agit dans le cadre de ses activités professionnelles ou d'entreprise, la Banque veillera uniquement à rectifier, sur le compte concerné, le montant de l'opération concernée.

12.5. La responsabilité invoquée dans le présent article n'est pas engagée lorsqu'une opération de paiement initiée via mobile banking n'est pas exécutée ou n'est pas correctement exécutée suite à la force majeure ou suite au respect d'une obligation issue d'une législation nationale ou européenne.
Sont notamment considérés comme cas de force majeure: guerre, émeutes, terrorisme, conflits sociaux, hold-up, incendie, inondation et autres catastrophes naturelles, défauts techniques graves ou autres catastrophes, désorganisation passagère des services postaux ou grève de la poste.

12.6. La Banque ne peut être tenue responsable de perturbations ou interruptions de la fonctionnalité mobile banking qui ne lui sont pas imputables. Elle ne peut non plus être tenue responsable des interruptions temporaires de la fonctionnalité mobile banking pour cause de maintenance, d'amélioration ou de sécurisation de celle-ci.

12.7. Le client supporte personnellement les conséquences du non-fonctionnement ou du mauvais fonctionnement de l'appareil qu'il utilise ainsi que de l'incompatibilité éventuelle de l'application mobile banking avec l'appareil du client.

La Banque ne peut en aucun cas être mise en cause en raison de perturbations, manquements ou fautes dus au fournisseur de l'appareil ou à n'importe quel tiers qui interviendrait dans la transmission ou la communication.

Article 13: Droits de propriété intellectuelle

Les droits de propriété intellectuelle relatifs à mobile banking appartiennent à la Banque et, le cas échéant, à ses fournisseurs, et ne seront en aucune façon et dans aucune mesure cédés au client. Le client respectera lui-même ces droits et les fera respecter par toute personne dont il répond. Il utilisera l'application et la documentation relative à mobile banking exclusivement pour ses propres besoins et ne les copiera pas, ne les mettra pas à la disposition d'un tiers quelconque et ne les diffusera pas. Il est bien entendu interdit au client d'apporter une modification quelconque à l'application mobile banking.

Article 14: Traitement des données à caractère personnel

Le traitement des données à caractère personnel dans le cadre de mobile banking est conforme à la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard du traitement des données à caractère personnel, comme prévu à l'article 1.9. du Règlement général des opérations.

Lors de l'utilisation par le client de mobile banking, certaines données personnelles, appelées ''variables d'environnement'', sont transmises à la Banque et enregistrées par elle via l'appareil du client:
• son adresse TCP/IP (numéro d'identification de l'appareil dont dispose le client sur le réseau Internet),
• les marques et versions de l'appareil utilisé ainsi que de son système d'exploitation,
• le numéro de série de l'appareil utilisé (UDID),
• la langue utilisée par le client,
• les pages des services mobile banking consultées par le client.

La Banque traite ces données en vue de pouvoir tenir compte des éléments propres à la configuration de l'appareil dont dispose le client afin de pouvoir lui envoyer les pages internet demandées dans un format adapté. Elles sont en outre traitées pour établir des statistiques de mobile banking et pour veiller à l'amélioration du contenu de ce service. Ces données ne sont pas utilisées pour identifier le client personnellement.

Article 15 : Tarifs

L'accès à, et l'usage de mobile banking sont gratuits, sans préjudice de la tarification de la carte bancaire AXA, du lecteur de carte et de certaines opérations conformément à la liste des tarifs de la Banque. Dans le respect de la procédure décrite ci-dessous en matière de modification du présent règlement, la Banque peut à l'avenir soumettre l'accès à et/ou l'usage de mobile banking au paiement d'une indemnité.
Les frais de télécommunication sont toujours à charge du client, de même que les frais de sa connexion Internet et de son abonnement auprès du prestataire de services Internet. Le client supporte également tous les frais relatifs à son appareil.

Article 16: Résiliation de l'accès au mobile banking

16.1. La convention relative à la fonctionnalité mobile banking est conclue pour une durée indéterminée.

16.2. Le client peut mettre fin à tout moment et sans frais au droit d'utilisation de mobile banking en supprimant ou en bloquant (faisant bloquer) l'application sur son appareil.

Le client peut mettre fin au droit d'utilisation de mobile banking accordé à un tiers pour son compte. Le client se charge lui-même de la notification de la résiliation audit tiers.

Si le client résilie son droit d'utilisation de homebanking conformément aux dispositions du Règlement homebanking, il résilie automatiquement son droit d'utilisation de mobile banking.

16.3. La Banque peut également mettre fin au droit d'utilisation de mobile banking moyennant une résiliation écrite adressée au client. Elle respectera à cet effet un délai de préavis de deux mois, sans préjudice du droit dont elle dispose de bloquer l'accès au mobile banking, comme prévu à l'article 8.1.5°.

La Banque peut en revanche mettre fin au droit d'utilisation du mobile banking, sans respecter ce préavis, si le client ne respecte pas ses obligations reprises dans les contrats et règlements applicables, en cas de négligence grave, faute lourde ou dol de la part du client, ou si certaines dispositions légales obligent la Banque à mettre fin à la relation avec le client avec effet immédiat.

Si la Banque met fin au droit d'utilisation de homebanking conformément au Règlement homebanking, il est automatiquement mis fin au droit d'utilisation de mobile banking.

16.4. Le cas échéant, les frais afférents au mobile banking portés en compte au préalable seront remboursés prorata temporis par la Banque à partir du mois suivant la résiliation de la convention. Les frais dus à terme échu seront portés en compte au moment de la résiliation, à concurrence du nombre de mois écoulés.

16.5. Le droit d'utilisation de mobile banking prend fin de plein droit dès que les relations d'affaires du client avec la Banque prennent fin et dans tous les cas dès que le client n'est plus lui-même titulaire ou cotitulaire d'aucun compte auprès de la Banque.

Article 17: Modification du règlement

17.1. Les dispositions du présent règlement et de la liste des tarifs d'application peuvent toujours être modifiées par la Banque.

17.2. Ces éventuelles modifications n'entrent en vigueur qu'après l'expiration d'un délai de 2 mois au moins, après que la Banque a informé le client de la modification prévue, soit par écrit, soit sur un support durable mis à la disposition du client.

Ce dernier peut décider, dans ce délai de deux mois, de résilier immédiatement et sans frais son contrat relatif au service mobile banking et en informer la Banque, auquel cas le droit d'utiliser mobile banking par lui et/ou pour son compte prend irrémédiablement fin à l'expiration de ce délai.

À défaut d'une telle résiliation par le client dans ce délai, il est irréfutablement réputé avoir accepté les modifications, qui lui sont dès lors immédiatement opposables.

17.3. Lorsque des fonctionnalités ou des services sont ajoutés à mobile banking, le client est informé au préalable des dispositions supplémentaires introduites dans le règlement et, le cas échéant, dans la liste des tarifs. Le client est réputé souscrire aux nouvelles dispositions dès qu'il utilise la fonctionnalité ou le service concerné.