AXA Bank Belgium fait partie du Groupe Crelan

RÈGLEMENT AXA MOBILE BANKING
Annexe 6 au Règlement Général des Opérations
28/03/2022

Ce règlement régit les droits et obligations du client comme de la Banque en ce qui concerne l'accès à et l'utilisation de AXA mobile banking (ci-après «mobile banking»).
Les présentes dispositions font partie intégrante des annexes au Règlement Général des Opérations d'AXA Bank Belgium. 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.

Sans préjudice d'autres lois et arrêtés, les opérations de paiement et d'investissement] via mobile banking sont régies respectivement par les dispositions de la législation relatives aux services de paiement repris dans le Livre VII Code de Droit Economique et la loi du 2 août 2002 relative à la surveillance du secteur financier et aux services financiers. Dans le présent règlement, il n'est pas dérogé aux dispositions impératives de cette législation. Les dispositions de cette loi reprises dans le présent règlement doivent dès lors être lues et interprétées comme telles.

À la suite de l'activation du service mobile banking, un exemplaire du présent règlement est fourni au client et il donne explicitement son accord avec son contenu et son application.

Le présent règlement est disponible en français et en néerlandais. Pendant la durée de la relation contractuelle relative au mobile banking, la Banque communiquera avec le client dans la langue indiquée lors de l'entrée en relation et ainsi consignée dans ses systèmes, étant entendu que certains communications ou documents ne seront faits, envoyés ou mis à disposition uniquement en néerlandais ou en français.

Le client a à tout moment le droit de demander une version du présent règlement sur support durable à la Banque.

Article 1: Définitions

-[la Banque: AXA Bank Belgium SA, dont le siège social est sis en Belgique, Boulevard Sylvain Dupuis 251, 1070 Anderlecht et titulaire du n° BCE/TVA BE 0404 476 835 RPM Bruxelles;][modifié le 28 mars 2022]

- le client: toute personne physique qui a activé l'accès à mobile banking et qui utilise le service mobile banking.
La Banque considère tous les clients qui consultent ou introduisent des transactions d'investissement via mobile banking ou pour lesquels des transactions d'investissement sont consultées ou introduites comme des clients non-professionnels (ou clients retail) qui bénéficient de la plus haute protection. Les clients ne peuvent pas opter pour une autre catégorie de clients.

- mobile banking: un ensemble de procédures, convenues avec le client, qui ouvrent l'accès aux services de mobile banking par l'intermédiaire d'un appareil du client permettant de gérer ses affaires bancaires en ligne à distance.

- Etats membres de l'UE: les états membres de l'Union Européenne, à savoir l'Allemagne, Autriche, Belgique, Bulgarie, Chypre, Croatie, Danemark, Espagne (y compris les Îles Canaries, Ceuta et Melilla) Estonie, Finlande, France (Guyane française, Guadeloupe, Martinique et Réunion inclus), Grèce, Hongrie, Irlande, Italie, Lettonie, Lituanie, Luxembourg, Malte, Pays-Bas, Pologne, Portugal (y compris Açores et Madère), République tchèque, Roumanie, Slovénie, Slovaquie, Suède.

- 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 du Single European Payment Area, à savoir les états membres de l'EEE + Suisse, Monaco, San Marino, Andorre, Royaume Uni (Gibraltar inclus), Ile de Man, Jersey, Guernsey, Cité du Vatican

- zone Euro: les états qui utilisent l'euro, à savoir l'Allemagne, Autriche, Belgique, Chypre, Espagne (y compris les Îles Canaries, Ceuta et Melilla), Estonie, Finlande, France, Guyane française, Grèce, Guadeloupe, Irlande, Italie, Lettonie, Luxembourg, Lituanie, Malte, Martinique, Pays-Bas, Portugal (y compris Açores et Madère), Réunion, Slovaquie, Slovénie

- homebanking: une fonctionnalité de la carte de débit AXA que le client peut activer et qui consiste en un ensemble de procédures lui permettant de gérer en ligne à distance ses affaires bancaires via un PC ou autre appareil ; son utilisation est régie par le Règlement homebanking; le client a reçu le présent règlement, en a pris connaissance au préalable 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.axabank.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.

- itsme : une application avec identifiant numérique pour les appareils mobiles Android ou iOS, que le client installe sur son appareil avec une fonction d'enregistrement, de login et de signature.
L'utilisation de itsme est régie par 'les Conditions Générales Application itsme' que le client accepte lors de la création de son compte itsme et qu'il peut retrouver sur le site web de

Belgian Mobile ID SA . itsme® est une application proposée par Belgian Mobile ID SA (www.belgianmobileid.be) avec son siège social Place Sainte-Gudule 5, 1000 Bruxelles, Belgique (n° BCO 541. 659.084, n° de TVA BE541 659 084)

- code itsme : le code d'identification personnel et secret composé de 5 chiffres avec lequel le client est tenu de s'identifier afin de pouvoir accéder à son compte itsme.

- empreinte digitale : l'empreinte du sillon de lignes du bout du doigt qui est laissée due à la couche graisseuse naturelle présente sur la peau.
Si le client a enregistré sa/ses empreinte(s) digitale(s) dans le système d'exploitation de son appareil, il peut également choisir d'utiliser la/les empreinte(s) digitale(s) comme moyen d'accès et de signature dans homebanking et mobile banking.

- reconnaissance faciale (faceID): la vérification, au moyen d'un système caméra sur les appareils qui en sont équipés, des mesures et autres caractéristiques spécifiques du visage. Si le client a enregistré son visage de telle manière dans le système d'exploitation de son appareil, il peut également décider d' utiliser la reconnaissance faciale comme moyen d'accès et de signature dans mobile banking.

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

- opération (de paiement) à distance: opération (de paiement) initiée par internet ou au moyen d'un appareil de communication à distance compatible, comme par exemple une opération de paiement via mobile banking.

- ordre (de paiement): demande ou ordre à la Banque initié par le client d'effectuer une opération de paiement ou autre transaction via mobile banking.

- opération d'investissement: ordre d'achat ou de vente de titres (marché secondaire) ou de souscription à des émissions (marché primaire) initié par le client via mobile banking en vue de son exécution (directe ou indirecte) par la Banque.

-services d'investissement: les services rendus par la Banque tels qu'exposés dans le règlement des services d'investissement.

- titres: instruments financiers au sens de la loi du 2 août 2002 relative à la surveillance du secteur financier et aux services financiers.

- identifiant unique: le numéro de compte qui doit être fourni, le cas échéant, par le client afin d'identifier sans équivoque le(s) numéro(s) de compte concerné(s) lors d'une opération de paiement en format IBAN (International Bank Account Number) pour les opérations de paiement au sein de la zone SEPA en euro.

- la carte t: la carte de débit AXA au nom du client régie par le Règlement carte bancaire AXA.

- lecteur de carte: un appareil (Unconnected Card Reader) certifié EPCI qui, en combinaison avec la carte et le code secret personnel, génère un code qui permet au client de s'identifier ou de signer des ordres.

- virement : opération de paiement où le client donne instruction à sa banque de débiter un compte à vue au profit du bénéficiaire spécifié indiqué dont le compte sera crédité.

- virement en euros : un virement en euros au sein de la zone SEPA

-virement instantané : un virement électronique individuel en euros qui est possible sous certaines conditions 24 heures par jour, 7 jours par semaine (24/7/365) entre les banques participantes et qui est exécuté immédiatement ce qui fait que les fonds virés sont effectivement disponibles en queques secondes sur le compte bénéficiaire.

- authentification : procédure permettant à la Banque de vérifier l'identité du titulaire de carte ou la validité de l'utilisation d'une carte de débit AXA, y compris les données de sécurité personnalisées.

- authentification forte du client : authentification reposant sur l'utilisation de deux éléments ou plus appartenant aux catégories 'connaissance' (ce que le client sait), 'possession' (ce que le client possède) et 'inhérence' (ce que le client est) et indépendants en ce sens que la compromission de l'un ne remet pas en question la fiabilité des autres, et qui est conçue de manière à protéger la confidentialité de données d'authentification.

- support durable: tout instrument permettant au client et/ou titulaire de carte de stocker les informations qui lui sont personnellement adressées d'une manière telle que ces informations puissent être consultées ultérieurement pendant une période raisonnable adaptée à leur finalité et reproduites à l'identique.

- 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.axabank.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.

- selfservice: automates bancaires installés dans les agences de la Banque qui permettent au client ou titulaire de carte d'effectuer lui-même des opérations bancaires sur ses comptes à vue, comptes à vue start2bank et comptes d'épargne tenus en euros ; ce service est en principe accessible 7 jours sur 7, de 06h à 22h ; pour des raisons de sécurité, l'espace selfservice peut faire l'objet d'une surveillance permanente par caméra.

Article 2: Description de la fonctionnalité mobile banking

2.1. 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 la nuit du dimanche de 3h00 à 4h00 et exceptionnellement du samedi soir 22h jusqu'au dimanche matin 6h).
L'application sera différente, suivant l'appareil sur lequel mobile banking est installé.

2.2. En vue d'assister le client lors de l'installation et l'utilisation de mobile banking, la Banque met à la disposition du client dans homebanking et sur le site internet de la Banque une liste détaillée de questions posées fréquemment. En plus, à plusieurs endroits dans mobile banking, il y des icônes informatives qui donnent les explications nécessaires au client. Si le client aurait encore des questions, il peut s'adresser à Customer Care au n° 03/266.66.55. ou envoyer un mail à edesk@axa.be.

Article 3: Accès, identification, signature et sécurisation

3.1. Pour pouvoir accéder au mobile banking, le client, qui satisfait aux conditions stipulées par la Banque, doit soit avoir déjà activé la fonctionnalité homebanking, comme spécifié dans le Règlement homebanking, soit avoir activé l'accès aux canaux digitaux (homebanking et mobile banking) lors de son premier enregistrement dans mobile banking ou lors de sa première connexion à homebanking, comme défini 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, en la téléchargeant du magasin d'application.

Il doit ensuite s'**enregistre**r une fois dans l'application mobile banking de l'appareil.

Le client doit disposer à cet effet :
- soit du lecteur de carte, de la carte et du code secret attribué à la carte
- soit de itsme®..

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

Lors de ce processus d'enregistrement, le client peut également choisir d'utiliser son **empreinte digitale** ou reconnaissance faciale (faceID) comme moyen d'accès et de signature pour mobile banking, si son appareil le permet.

Si le client n'a pas encore enregistré son empreinte digitale ou la reconnaissance faciale (faceID) sur son appareil lors de la première connexion, il peut, s'il le souhaite, enregistrer sa (ses) empreinte(s) digitale(s) ou la reconnaissance faciale (faceID) sur son appareil à un moment ultérieur pour pouvoir l'utiliser via mobile banking.

La Banque utilise seulement la lecture de l'empreinte digitale ou la reconnaissance faciale (faceID) comme moyen d'accès et de signature.
Des informations relatives à l'empreinte digitale ou à la reconnaissance faciale (faceID) ne sont enregistrées nulle part et ne sont pas utilisées à d'autres fins.
Pour plus d'informations à ce sujet, la Banque réfère le client au fabricant de l'appareil concerné.

La Banque peut (temporairement) désactiver le moyen d'accès et de signature par empreinte digitale ou par reconnaissance faciale (faceID) si c'est nécessaire, par exemple si les empreintes digitales ou la reconnaissance faciale (faceID) enregistrées sur l'appareil ont été modifiées ou si plus d'un utilisateur a été enregistré sur un appareil. Dans ce dernier cas, l'utilisation de l'empreinte digitale ou de la reconnaissance faciale (faceID) comme moyen d'accès et de signature ne sera pas possible pour des raisons de sécurité.

3.3. Pour utiliser mobile banking, le client peut faire appel aux **moyens d'accès et de signature** suivants :
-le code secret
-l'empreinte digitale
-reconnaissance faciale (faceID) – uniquement pour les appareils avec IOS comme système d'exploitation
-un clic sur le bouton de confirmation
-le lecteur de carte, la carte et le code secret qui l'accompagne
- itsme®

Le client peut se connecter dans mobile banking avec les **moyens d'accès** suivants :

-soit avec le code secret
-soit avec l'empreinte digitale
-soit avec la reconnaissance faciale (faceID) - uniquement pour les appareils avec IOS comme système d'exploitation.

Le client peut signer ou confirmer des ordres de paiement et d'investissement et d'autres ordres, actions et demandes qu'il initie via mobile banking avec **les moyens de signature** suivants :
-soit avec son code secret
-soit avec son empreinte digitale
-soit avec la reconnaissance faciale (FaceID) – uniquement pour les appareils avec IOS comme système d'exploitation
-soit avec le lecteur de carte, la carte et le code secret qui l'accompagne si une seconde signature est demandée.
- soit avec itsme®

Le cas échéant, pour des raisons de sécurité, le client sera tenu tenu de signer certains ordres une deuxième fois avec un des moyens de signature.

Le client reconnaît ces moyens d'accès et de signature comme constitutifs de sa signature électronique, qui répond à toutes les exigences légales en matière d'authentification forte de client.

Pour certaines actions dans mobile banking, un clic sur un bouton de confirmation suffit comme confirmation. Le client reconnait ainsi avoir donné son autorisation pour ces actions.

Le cas échéant, le client sera tenu de signer certains ordres une deuxième fois avec un des moyens de signature, pour des motifs de sécurité.

Lorsque le client utilise 5 fois de suite un code secret erroné dans mobile banking, la Banque bloque l'accès

au mobile banking. Le client peut faire débloquer l'accès via le contacl center de la Banque. [Il peut également débloquer l'accès en exécutant un nouvel enregistrement dans mobile banking.

Si le client a oublié son code secret, il devra faire un nouvel enregistrement et il pourra alors enregistrer un nouveau code secret. Il peut également à tout moment passer à l'empreinte digitale ou FaceID, si disponible.][modifié le 14 juin 2021].

Lorsque l'empreinte digitale du client est refusée 5 fois de suite, il doit introduire le mot de passe de son système d'exploitation. Il peut également à tout moment passer à son code secret.

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

3.4. AXA Mobile Sign :
Mobile Banking dispose d'une fonctionnalité qui permet au client de s'identifier et de s'authentifier dans mobile banking et de signer des ordres et demandes avec les moyens d'accès et de signature, dont le code secret, l'empreinte digitale et la reconnaissance faciale, via l'appareil sur lequel il a installé mobile banking.
Le Règlement homebanking y réfère sous le nom AXA Mobile Sign.

3.5. Les moyens d'accès et de signature sont strictement personnels et confidentiels.
La sécurité d'utilisation maximale pour le client n'est rendue possible que par leur utilisation discrète et simultanée.

3.6 Pour les mineurs d'âge et autres cas incapables, l'accès à mobile peut être limité en application ou non des instructions données à la Banque à cet égard

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 par l'intermédiaire de son appareil.
L'utilisation effective des différentes fonctionnalités de mobile banking ne peut être limitée qu'en vertu des dispositions du présent règlement.

Dès que le client est connecté dans mobile banking, il peut voire une page 'Nouvelles'.
Cette page sera seulement présentée si une nouvelle version de l'application mobile banking a été installée, et elle reprend les modifications les plus récentes et/ou les nouveautés de mobile banking.

4.1. Comptes et cartes

4.1.1. Comptes

4.1.1.1 Aperçu

Le client peut, via cette option menu 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. Le cas échéant, il sera affiché à côté du solde à un moment défini, le solde dont dispose le client effectivement pour encore effectuer des paiements. Ce dernier solde tient également compte des montants éventuellement réservés pour des opérations déjà effectuées mais non encore comptabilisées sur le compte et/ou d'une ouverture de crédit autorisée sur le compte concerné.

[La Banque peut toujours décider que certains comptes ne seront pas consultables ou accessibles via mobile banking.][modifié le 1er janvier 2022]

Les comptes soldés et les comptes bloqués ne s'affichent pas.
Pour les mineurs d'âge ou les mandataires qui ne sont pas titulaires ou cotitulaires, cette possibilité peut être limitée, en application ou non des instructions données à la Banque à cet égard par des personnes habilitées à le faire.

Via homebanking, le client majeur et capable peut déterminer, par appareil sur lequel mobile banking est activé, quels comptes il souhaite pouvoir consulter et utiliser.

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.
Via un icone de recherche, certaines transactions peuvent être recherchées sur base de par exemple le montant, le bénéficiaire, la date et la description.

[ ][supprimé le 1er janvier 2022]

En cliquant sur un numéro de compte, le client peut partager ce numéro avec des tiers (share account number).

Le cas échéant, le client recevra en outre des transactions effectuées, également une liste des transactions futures et des transactions refusées.

Le client verra également le nom compte qu'il aura éventuellement donné à un compte (rubrique). Ce nom compte n'est pas utilisé comme nom du donneur d'ordre sur un ordre de virement, mais vise uniquement à aider le client à reconnaître plus facilement ses comptes (rubrique). La Banque ne peut être tenue responsable des erreurs qui pourraient se produire par suite de l'utilisation de tels noms comptes. Le client peut à tout moment modifier ou supprimer un nom compte via son agence.
Le client peut à tout moment ajouter, modifier ou supprimer un tel nom compte.

Via un bouton action, le client qui est titulaire d'un compte à vue start2bank, régi par Règlement compte à vue start2bank, pourra convertir son compte à vue start2bank vers un compe à vue confort2bank, régi par le Règlement comptes à vue. A cet effet, le client pourra introduire via mobile banking toutes les données indispensables et parcourir tout le procédé de conversion.

4.1.1.2 Virements en euros

Le client peut, via le bouton action prévu à cet effet, introduire des ordres de virement en euros, suivant les limites définies à l'article 6.

Lorsque le client introduit un ordre de virement vers un bénéficiaire qui n'est pas encore sauvegardé, il peut sauvegarder ce bénéficiaire lors de l'introduction de l'ordre de virement, comme dans homebanking, avant de signer la transaction.
Le client peut gérer la liste de bénéficiaires qu'il a créée dans l'option menu 'plus' comme défini à l'article 4.4. ou via homebanking, comme défini dans le règlement homebanking.

Les virements qui exigent plus d'une signature et qui sont introduits via mobile banking, seront refusés.

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

Si le client est mineur d'âge (12-17j), il ne peut pas effectuer de virements avec un compte d'épargne comme compte donneur d'ordre.
Pour les personnes majeures, cette possibilité est limitée conformément aux conditions et modalités d'application sur les comptes d'épargne.

Chaque ordre de virement doit être signé séparément et transmis à la Banque. Le client reconnaît la validité légale des ordres de virementt qu'il a donnés, comme décrit à l'article 7.

Après l'avoir introduit, le client peut envoyer l'ordre de virement par courrier électronique afin de fournir la preuve de l'instruction donnée. Toutefois, ce courriel ou une impression de celui-ci ne constitue 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.

4.1.1.2.1. Pour ce qui concerne **les ordres de virement qui ne sont pas des virements instantanés**, les dispositions suivantes s'appliquent, sans préjudice à l'article 8.1.4° :
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 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 de débit AXA, telles qu'elles figurent dans le Règlement carte de débit AXA.

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.

Une date d'exécution dans le futur doit se situer dans le futur, avec un maximum d'un an. Le client peut aussi annuler les virements en euros enregistrés avec une date d'exécution dans le futur ou modifier cette date. A cet effet, une signature est toujours nécessaire avec un des moyens de signature, tel que décrit à l'article 3.

Le client peut choisir d'exécuter un virement une fois ou à plusieurs reprises. Dans ce dernier cas, le paiement sera ajouté à la liste de paiements automatiques.

4.1.1.2.2**. Pour les virements instantanés**, contrairement aux dispositions de l'article 4.1.1.2.1. et du règlement relatif à la carte de débit AXA, les dispositions suivantes sont d'application :

Les ordres de virement instantanés ne sont possibles qu'à partir de certains comptes à vue, pour autant que toutes les conditions des virements instantanés soient remplies.

Ces paiements flash ou en temps réel seront exécutés immédiatement, 24/7/365, y compris les jours fériés et les jours non bancaires.

Il n'est par définition pas possible d'indiquer une date d'exécution souhaitée dans le futur.

Lors de l'introduction d'un ordre de virement individuel, le client indique lui-même s'il souhaite que celui-ci soit exécuté sous forme de virement instantané. Les virements instantanés sont toujours ponctuels.

Si le solde disponible est insuffisant, l'ordre de virement instantané est immédiatement refusé et non présenté, comme c'est le cas pour les autres ordres de virement, cinq jours ouvrables bancaires sur le compte. Dans ce cas, le client sera informé d'un tel refus dans un délai très court par le biais d'une notification.

4.1.1.3. Ouverture compte d'épargne

Via le bouton action +, s'il est présent, le client peut ouvrir un nouveau compte d'épargne.

La Banque détermine quels comptes d'épargne, pendant quelle période, sont disponibles pour être ouverts via mobile banking. Cette offre peut varier de jour à jour.

Le client est tenu de lire toute l'information (dont règlements et liste des tarifs) mis à disposition et se déclare explicitement d'accord avec les dispositions qui y sont stipulées par sa signature avec un des moyens de signature, comme définis à l'article 3 de ce règlement.

Les documents mentionnés ci-dessus peuvent toujours être téléchargés gratuitement sur son appareil.

Il est possible que le produit ouvert n'apparaisse pas immédiatement dans l'aperçu des comptes pour des raisons techniques. Ce compte sera pourtant disponible en tant que bénéficiaire d'un virement. Ce virement sera visible dans la liste 'transactions provisoirement refusées' jusqu'à son exécution définitive.

4.1.1.4. Zoomit

Via cette option, le client qui a activé le service Zoomit via homebanking et qui y est habilité, peut consulter les factures électroniques avec comme statut 'restant à payer' et s'il le souhaite il peut les payer directement. Ces paiements sont traités comme les autres ordres de virement.
Zoomit est un service facultatif, dont les conditions d'utilisation sont reprises à l'article 5 du règlement homebanking.

4.1.1.5. Demandes en cours

Si la signature du client est requise pour l'ouverture d'un produit, alors une liste des demandes apparaîtra ici. Par demande le client peut opter de consulter, approuver ou refuser cette demande.

4.1.1.6. Payconiq by Bancontact

Avec Payconiq by Bancontact, le client peut rapidement et simplement effectuer des paiements avec son smartphone dans un magasin ou entre amis ou famille. Si le client télécharge l'application Payconiq by Bancontact et opte pour des paiements directs de son compte à vue auprès de la Banque, il est tenu de lier ce compte à vue à l'application. Partant de l'application Payconiq by Bancontact et selon la manière qui y est définie, le client sera redirigé vers AXA Mobile Banking. Le client choisit ensuite le compte à vue qu'il souhaite lier, confirme son choix et sera ensuite en mesure d'effectuer des paiements avec le compte choisi via Payconiq.

Des paiements initiés par Payconiq by Bancontact sont des ordres de virement ou des paiements par carte qui entraînent le débit du compte à vue lié. Ils sont régis par les disopsitions du Règlement comptes à vue et carte de débit AXA.

4.1.2. Cartes

Via l'option menu 'Cartes', le client peut consulter un aperçu de la (les) carte(s) de débit et de crédit dont il est personnellement titulaire.

4.1.2.1. Cartes de débit

Par carte de débit, le client peut consulter plusieurs détails et gérer certaines fonctionnalités (telles décrites dans le Règlement carte de débit AXA) liées à sa carte.
[Le cas échéant, le client qui en a le droit, peut demander le remplacement de sa carte de débit AXA. La décision concernant cette demande sera prise par les services centraux de la Banque et sera communiquée au client.][modifié le 1er janvier 2022]

4.1.2.2. Cartes de crédit

Le client peut, via cette option consulter un relevé de la (des) carte(s) de crédit AXA portant le logo VISA, dont il est personnellement le titulaire ou qui est/sont lié(s) à/aux compte(s) à vue dont il est le titulaire principal (le titulaire principal d'un compte est le seul titulaire ou lorsqu'il y a plusieurs titulaires, celui qui est introduit dans les systèmes de la Banque comme premier titulaire du compte en question.)

Partant de la limite de dépenses, attribuée au titulaire et liée à la carte de crédit, consulter la somme déjà utilisée de la limite de dépenses pour la période de facturation en cours et si le client clique plus loin, il pourra également consulter le solde encore disponible 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 Worldline au n° 02/205.85.85.

Par carte de crédit, le client peut ensuite consulter des informations sous les options-menu 'Historique' et 'Paramètres'.

*Historique

Via l'onglet 'dépenses courantes', il peut consulter un relevé des opérations de paiement qu'il a effectuées avec cette carte depuis la dernière facturation des transactions, communiquées via le dernier relevé de comptes.

Via l'onglet 'relevé de dépenses, il peut consulter consulter un récapitulatif de tous les relevés de dépenses avec les transactions des 18 derniers mois, sauf si le titulaire principal, comme défini ci-avant, a opté de recevoir les relevés de dépenses sur papier. Chaque relevé de dépenses peut être ouvert séparément.

Les informations que le client/titulaire de carte peut consulter via ces onglets sont souvent mises à disposition par des tiers, comme stipulé à l'article 5, qui est donc invariablement d'application.

Via un bouton, le client qui y est habilité et qui répond à toutes les conditions, et à condition que la carte demandée est liée à un compte à vue pris en compte à cet effet peut demander une carte de crédit VISA, régie par le Règlement cartes de crédit. Le client peut introduire toutes les données requises via mobile banking.
La décision quant à cette demande est prise par les services centraux et sera communiquée au client par e-mail.

*Paramètres

Via ce menu, le client peut gérer certaines fonctionnalités liées à sa carte de crédit.

4.2. Investissements

4.2.1. Comptes-titres

4.2.1.1. Via l'option menu 'Investir soi-même' le client reçoit un aperçu de tous ses comptes-titres. L'aperçu montre pour chaque compte-titres la valeur globale (en euros) de tous les titres sur le compte-titres, au dernier cours connu du jour bancaire ouvrable précédent.

Selon le type de compte-titres : 'investir seul', 'investir avec service' et 'investir avec service privilege', le client reçoit également plus d'informations concernant les services d'investissement et les services annexes qui y sont liés, avec différentes présentations graphiques.

Outre la valeur globale, le client reçoit également un aperçu de la valeur de chaque type de titre (action, obligation, fonds…) et pour chaque catégorie de titre séparément, aussi bien en EUR qu'en %.

Si le client clique sur un titre spécifique, il reçoit des informations concernant ce titre, dont un graphique avec l'évolution du cours (si disponible), la valeur actuelle, la valeur d'achat, le rendement éventuellement possible… .

4.2.1.2 Via le menu 'Historique', le client reçoit par compte-titres un aperçu des transactions (transactions d'investissement, transactions exécutées et en cours et versements de dividendes et intérêts). Si le client clique sur une transaction spécifique, il verra plus de détails concernant cette transaction.

4.2.1.3. Via le menu 'rapports' la Banque met à la disposition du client des relevés de titres et des relevés de tous les coûts et charges liés aux services d'investissement et aux titres sur son compte-titres

4.2.1.4 A plusieurs endroits dans mobile banking, le client peut ouvrir un compte-titres.

Chaque compte-titres ouvert via mobile banking sera censé être un compte-titres du type 'investir seul'. Mais dès que ce compte-titres et plus particulièrement dès que les titres détenus sur ce compte-titres font partie du conseil en investissements donné par l'agent, comme décrit dans le règlement des services d'investissement, la Banque considère ce compte-titres comme un compte-titres du type 'investir avec service'.

Les comptes-titres du type 'investir avec services privilege' ne peuvent pas être ouverts via mobile banking. Dans ce cas, le client doit se rendre à l'agence.

Le client est tenu de lire toute information et règlements mis à disposition et de déclarer explicitement son accord avec les dispositions qui y sont stipulées par sa signature avec les moyens de signature, comme définis à l'article 3 de ce règlement. Les documents mentionnés ci-dessus peuvent toujours être téléchargés gratuitement et sauvegardés sur son appareil et/ou imprimés.

L'ouverture d'un compte-titres nécessite le lien avec un (autre) compte déjà ouvert. Seulement les comptes, sur lesquels le(s) titulaire(s) peut (peuvent) agir seule(s), peuvent être liés à ce nouveau compte-titres.

Si l'ouverture d'un compte via mobile banking requiert la signature d'une 2ème personne (non-demandeur), le compte sera seulement effectivement ouvert lorsque le non-demandeur également aura signé avec les moyens de signature, comme définis à l'article 3 de ce règlement.

Il est possible que le compte ouvert n'apparaît pas immédiatement dans l'aperçu des comptes pour des raisons techniques. Des transactions d'investissement ne sont pas encore possible sur ce compte.

4.2.1.5. Via le l'option menu 'Ouvrir votre plan d'investissement'/'Gestion de votre plan d'investissement', le client peut ouvrir et/ou adapter un plan d'investissement. Les modalités de fonctionnement relatives au plan d'investissement, telles que définies dans le règlement des services d'investissement, sont intégralement d'application, sauf si les dispositions mentionnées ci-dessous y dérogeraient.

Avant que le client puisse passer à l'ouverture effective d'un plan d'investissement, il en reçoit une description exhaustive, un planning des étapes à suivre pour démarrer le plan d'investissement, un relevé des fonds que le client peut sélectionner et des informations élaborées par fonds.

Le client qui clique sur l'écran 'achat via plan d'investissement' arrive sur l'écran où il choisit un montant à investir, la fréquence à investir, la date de départ et la date de fin.
Si le client n'a pas encore de compte-titres au moment de l'ouverture du plan d'investissement, il pourra également ouvrir un compte-titre lors du processus d'ouverture. Le cas échéant, les mêmes modalités qui sont reprises à l'article 4.2.1.4. de ce règlement sont d'application.

Les achats via le plan d'investissement via le compte-titres 'investir avec service privilege' sont uniquement possibles sous la forme d'achats en plus du titre (fonds) que le client détient déjà sur le compte-titres mentionné.

La Banque n'offre pas de conseil en investissement, ni concernant l'ouverture du plan d'investissement via mobile banking, ni sur le choix des fonds et les modalités du plan d'investissement via mobile banking.

La Banque n'offre pas de conseil en investissements, ni sur l'ouverture du plan d'investissement via mobile banking, ni sur le choix des fonds et des modalités du plan d'investissement via mobile banking. La Banque considère l'ouverture du plan d'investissement et le choix des fonds dans ce plan comme une opération effectuée à la simple initiative du client. Avant que le client ne confirme l'ouverture (le choix des fonds inclus), il reçoit sur son écran un avertissement où il lit qu'il a effectué les transactions d'investissement de sa propre initiative, que la Banque n'a pas contrôlé l'adéquation des transactions d'investissement et que dès lors il ne bénéficie pas de la protection prévue par le contrôle d'adéquation. De plus, on attire son attention sur le fait que le Règlement des services d'investissement/tarifs dans la liste des tarifs sont d'application sur cette transaction et que la Banque lui a fourni diverses informations via mobile banking.

L'option 'aide' que le client peut consulter sans obligation lorsqu'il choisit son/ses fonds, mène le client vers un/des fonds spécifique(s) sur base des caractéristiques spécifiques liées aux fonds. Mais la Banque ne se prononce pas sur l'adéquation des fonds pour le client sur base de sa capacité financière, ses objectifs d'investissement et sa connaissance et expérience en matière d'investissements en fonds. Cette option aide ne peut donc pas être considérée comme conseil en investissements dans le sens du droit financier.
L'option 'aide' n'est pas à la disposition du client s'il veut réaliser des achats en plus du titre (fonds) qu'il détient déjà sur le compte-titres 'investir avec service privilege'.

Pour le reste, la Banque réfère aux dispositions concernant l'exécution pure et simple à l'initiative du client (execution only), comme définie dans le règlement des services d'investissement.

Aussi bien la(les) transaction(s) d'achat du titre que le message d'avertissement ci-dessus sont finalement confirmés par le client via signature avec un des moyens de signature, définis à l'article 3 de ce règlement.

Si par après le client souhaite modifier des éléments (par exemple le choix des fonds, le montant à investir, la fréquence d'épargne, la date de fin) de son plan d'investissement, ouvert via mobile banking ou s'il veut résilier le plan d'investissement, il peut le faire via homebanking et mobile banking.
Un plan d'investissement ouvert avec conseil en investissement chez l'agent, peut être consulté, modifié (montant d'investissement, fréquence d'investissement et date de départ et de fin) et résilié par le client via mobile banking .

L'exécution par la Banque de transactions d'investissement dans des fonds est effectuée selon la politique d'exécution, comme définie dans l'addendum 'Synthèse de la politique d'exécution et de transfert des ordres relatifs aux instruments financiers en vigueur chez AXA Banque pour les clients non professionnels.' du règlement des services d'investissement.

4.2.1.6. En outre, le client est en mesure de donner un nom au compte-titres. Ce nom sert uniquement d'outil personnel du client pour pouvoir distinguer ses divers

comptes les uns des autres, mais n'entraîne pas de conséquences judiciaires ni dans le chef de la Banque ni dans le chef de tiers.

4.2.2. Epargne-pension

Dans mobile banking, le client peut ouvrir un compte d''épargne-pension, comme décrit dans le Règlement des services d'Investissement, dont les modalités spécifiques sont intégralement d'application, sauf si les dispositions ci-après y dérogeraient.

La Banque ne donne pas de conseil en investissement ni sur l'ouverture du compte d'épargne-pension via mobile banking, ni sur le choix du fonds d'épargne-pension via mobile banking.

Avant que le client puisse procéder à l'ouverture en soi, il reçoit des informations exhaustives sur les 3 fonds d'épargne-pension parmi lesquels il peut choisir lui-même, une fiche explicative des caractéristiques de l'épargne-pension qui donne également un aperçu des coûts estimés et des charges liées à l'investissement dans un fonds d'épargne-pension.

Le client qui clique sur le lien 'demander' devra ensuite répondre à quelques questions afin que la Banque puisse vérifier s'il a suffisamment de connaissance et d'expérience sur les risques liées à l'épargne-pension/aux fonds d'épargne-pension.
Via l'écran, il sera informé du résultat de ce contrôle d'adéquation et le cas échéant, averti du fait que sa connaissance est insuffisante pour comprendre les risques liés à l'épargne-pension.

Si le client décide de démarrer avec l'épargne-pension, il devra dans les écrans qui suivent successivement :

1. Compléter et/ou confirmer ses données de contact, dont son adresse e-mail. Cette adresse sera utilisée pour :
   -aviser le client de l'ouverture de son compte d'épargne-pension
   -fournir au client un formulaire de demande en pdf signé électroniquement avec une présentation écrite des données introduites électroniquement par le client
2. Indiquer une agence pour la gestion
3. Indiquer un compte lié
4. Indiquer le type d'épargne (épargne automatique avec montant fixe ou immédiatement un premier versement)

Si le client choisit le plan d'épargne automatique, alors la somme à verser mensuellement sera calculée en fonction de la somme légale maximale qui peut être versée annuellement. En tous cas, la somme d'épargne annuelle sur le compte d'épargne-pension ne peut jamais dépasser le montant maximum légal.

Si le client opte pour un premier versement lors de l'ouverture du compte épargne-pension, il est lui-même responsable des virements ultérieurs à effectuer à temps si la somme légale maximale qui peut être versée annuellement n'a pas encore été atteinte.

A la fin, via signature avec un des moyens de signature, décrits à l'article 3, le client :

- confirmera son accord avec les points mentionnés ci-dessus
- confirmera que la Banque lui a avisé que le choix et l'ouverture du compte d'épargne-pension se passe sans conseil de la Banque et que la Banque l'a informé si l'épargne-pension est adéquate pour lui ou non.
- confirmera qu'il a reçu des informations importantes de la Banque et que la convention peut être exécutée immédiatement pendant le délai de renonciation.

le client peut à tout moment suspendre son plan d'épargne automatique pour l'épargne-pension et éventuellement effectuer des virements ultérieurs spontanément et sur sa propre responsabilité.

Via mobile banking, le client ne peut pas passer d'un fonds d'épargne-pension vers un autre fonds d'épargne-pension.

La transmission d'opérations d'investissement dans des fonds d'épargne-pension s'effectue selon la politique d'exécution, comme décrite dans l'a**nnexe:** Synthèse de la politique d'exécution et de transfert des ordres relatifs aux instruments financiers en vigueur chez AXA Banque pour les clients non professionnels du règlement service d'investissement.

4.3. Emprunts

Via l'option menu 'emprunter', le client peut :

- Consulter un aperçu de ses prêts demandés : il s'agit d'un aperçu des prêts à tempérament et des crédits-logement que le client a demandés à son agent, via homebanking ou via mobile banking.

- Consulter l'aperçu de ses crédits en cours : un aperçu de ses crédits-logement et prêts à tempérament dont il est (co)titulaire. Les crédits-logement avec une période de prélèvement encore en cours et les crédits contractés auprès de l'ancien Winterthur ne sont pas repris dans l'aperçu. Si le crédit a été contracté après le 17 janvier 2001, le client peut, en cliquant sur le numéro du crédit, consulter quelques détails du crédit en question.

- Consulter un aperçu de ses simulations sauvegardées : il s'agit d'un aperçu des simulations de prêts à tempérament et/ou de crédits logement effectuées pour le client par l'agent ou via homebanking ou mobile banking.

- Faire des simulations pour les différents types de prêts à tempérament (entre autres un prêt auto, un prêt de rénovation, un prêt energy@home ou un prêt personnel) et pour des crédits-logement (e.a. pour l'achat, la construction, la rénovation ou l'achat et la rénovation d'un logement). Ces simulations peuvent être sauvegardées si le client le souhaite. Elles restent visibles dans l'aperçu jusqu'à l'expiration de la date de validité. Faire une simulation ne garantit pas l'obtention du prêt. A ce moment-là, AXA Bank n'a encore aucun engagement.
Partant d'une telle simulation, le client peut demander un prêt à tempérament ou un crédit-logement. A cet effet, il doit passer par un certain nombre d'étapes, répondre à un certain nombre de questions, et dans de nombreux cas également télécharger un certain nombre de documents. Introduire une demande n'est pas une garantie d'obtenir le prêt. Ce n'est qu'après l'analyse de la demande que la banque décidera de fournir ou non une offre de crédit. Dans de nombreux cas, le processus de demande peut être finalisé complètement via mobile banking (c'est-à-dire jusqu'à la signature du contrat de crédit, et dans le cas d'un prêt à tempérament même la mise à disposition du montant de crédit). Dans certains cas, le client devra s'adresser à son agent bancaire AXA pour compléter la demande de crédit.

- Si le client est marié ou cohabite légalement, il ne peut faire une demande de prêt à tempérament qu'à son nom

avec celui du/de la partenaire concerné(e). Dans le cas d'un prêt à tempérament], le client a la possibilité de souscrire, avec le prêt, une assurance AXA Credit Protection (assurance décès-invalidité) d'AXA Belgium. Si une demande de prêt a été entièrement remplie, ce prêt disparaîtra de l'aperçu des «prêts demandés» et pourra être consulté dans l'aperçu des «prêts en cours» du client (à l'exception des crédits-logement avec une période de prélèvement encore en cours).

Après l'approbation du prêt par la banque, le client doit signer électroniquement un certain nombre de documents, dépendant du type d'emprunt, dans mobile banking.
Ces documents seront stockés pour le client dans sa boîte aux lettres digitale dans homebanking ou mobile banking pendant toute la durée du prêt.

Certains clients ne seront pas en mesure de demander un prêt à tempérament via mobile banking. Les raisons les plus importantes peuvent être:
* La Banque n'a pas enregistré de numéro de registre national pour ce client (ou pour sa/son partenaire);
* Le client (ou sa/son partenaire) a répondu positivement aux questions FATCA;
* une demande antérieure du client (ou de sa/son partenaire) a été refusée au cours des 6 derniers mois;
* Le client (ou sa/son partenaire) a moins de 18 ans ou plus de 75 ans;
* La Banque n'a aucun détail sur la carte d'identité du client (ou de sa/son partenaire) ou sa carte d'identité a expiré;
* Le client est marié ou cohabite légalement mais AXA ne connaît pas le/la partenaire;
* Le client est déjà séparé de fait mais encore marié officiellement;

Ces clients pourront uniquement soumettre une demande via leur agent bancaire AXA.

Pendant toute la durée du processus de demande de prêt, les règles décrites dans les conditions générales de crédit et dans le document «informations précontractuelles», et qui sont toujours disponibles via Mobile banking, s'appliquent.

4.4. Plus

4.4.1. Notifications

4.4.1.1. Notifications et Inbox

L'accès à et l'utilisation de la boîte postale digitale dans homebanking est également mis à disposition par la banque via mobile banking. Pour l'utilisation et les modalités de la boîte postale digitale, nous renvoyons au règlement homebanking.

[4.4.1.2. Notifications 'push'

Via ce menu le client peut :
-après avoir été invité à vérifier les réglages généraux de son appareil en matière de notifications, autoriser ou non que la Banque envoie des notifications 'push' sur son appareil via l'application mobile banking, comme défini à l'article 4.6.
-lire et/ou supprimer les notifications 'push' envoyées par l'app AXA mobile banking sur son appareil.][card stop le 1er janvier 2022]

4.4.2. Payer

4.4.2.1. Paiements automatiques

Via cete option menu, le client peut demander un aperçu de ses paiements automatiques. Au départ de cet aperçu, le client peut modifier, supprimer ou envoyer via e-mail un paiement automatique. Il peut également y ajouter un nouveau paiement automatique]

4.4.2.2. Payconiq

Via cete option menu, le client peut via un lien accéder à l'application Payconic by Bancontact et ainsi initier des paiements de son compte à vue lié.

Via ce menu, le client peut également consulter le compte à vue qu'il a lié à l'application Payconiq by Bancontact. S'il le souhaite, il peut annuler ce lien. S'il souhaite ensuite de nouveau initier des paiements via Payconiq by Bancontact, il devra rétablir le lien, comme défini à l'article 4.1.1.6.

4.4.3. Gestion des bénéficiaires

Via cette option menu, le client peut consulter un aperçu des bénéficiaires qu'il a sauvegardés et gérer cette liste. Il peut ajouter, modifier ou supprimer des bénéficiaires.

4.4.4. Gestion des cartes

Via cette option menu, le client peut gérer les préférences de ses cartes de débit et de crédit, comme défini à l'article 4.1.2.

4.4.5. AXA Mobile Sign

Via cette option menu le client peut utiliser les moyens d'accès et de signature dont il dispose en mobile banking, pour se connecter et s'authentifier et pour signer des ordres en homebanking, à l'aide de l'appareil sur lequel il a installé le service mobile banking.

4.4.6. Mes données

Via cette option menu, le client peut consulter et dans certains cas adapter :
- ses données personnelles
- ses données légalement obligatoires
- ses données de contact

moyennant la signature avec un des moyens de signature, comme définis à l'article 3. Certaines modifications demandent un examen plus approfondi et/ou une décision des services centraux de la Banque.

4.4.7. Préférences de mon app

Le client peut, via cete option menu modifier les préférences suivantes :
- son choix de langue
- son nom d'utilisateur
- son code pin
- s'il souhaite ou non utiliser son empreinte digitale (touchID sur iOS) ou reconnaissance faciale (faceID sur IOS) comme moyen d'accès et de signature. Ceci est uniquement possible si l'appareil sur lequel mobile banking est installé le permet.
- supprimer un utilisateur.
-[si l'utilisation de homebanking est bloquée pour lui, la débloquer

4.4.8. Contact

4.4.8.1. Vos agents bancaires AXA

Le client peut, via ce menu consulter les coordonnées de son (ses) agent(s) bancaire(s) AXA.

4.4.8.2. Agents bancaires et selfservice

Le client peut, via ce menu 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, équipés ou non d'un appareil self-service.

4.4.8.3. Contact

Le client reçoit, via ce menu, des informations sur:
- les coordonnées et l'accessibilité du customer care de la Banque,
- une démo présentant le fonctionnement de mobile banking.

4.4.8.4. FAQ

Via ce menu, le client peut consulter la liste avec les gestions fréquemment posées concernant mobile banking.

4.4.8.5. Card Stop

Via ce menu, 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 de débit AXA et cartes de crédit.

4.4.8.6. Débloquer homebanking

Via cette option menu, le client, pour qui l'utilisation de homebanking est bloquée, peut débloquer homebanking.

4.4.9. Information juridique

4.4.9.1. Conditions

Via ce menu, le client peut consulter le présent Règlement AXA Mobile Banking.

4.4.9.2. Ma Vie privée

Via ce menu, le client est dirigé vers la clause Privacy de la Banque, sur le site internet de la Banque.

4.4.10. Déconnecter

Via ce menu, le client peut clôturer la session de mobile banking.

[l'ordre des fonctionnalités repris dans l'article 4.4. a été modifié le 28 mars 2022]

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

Pour certaines fonctionnalités, le client ne doit pas se connecter:
- Il peut consulter une liste de tous les utilisateurs d'un certain appareil sur lequel mobile banking est installé, interchanger avec les différents utilisateurs qui ensuite peuvent se connecter personnellement.
- Un nouvel utilisateur peut être ajouté.
- Il peut via le menu 'aide' rechercher les données de contact de la Banque
- Il peut retrouver toutes les données de Cardstop, comme définies ci-avant.
- Il peut rechercher des agents bancaires AXA et des appareils self service, comme définis ci-avant.
- Via un lien, il peut être redirigé vers l'application Payconiq by Bancontact. Partant de là, il peut initier des paiements de son compte à vue lié

4.6. Notifications

Si le client en donne l'autorisation, la Banque enverra dans certains cas définis des notifications partant de l'application mobile banking vers son appareil, sans qu'il est tenu d'être connecté à mobile banking (les notifications 'push'). Ainsi, le client peut recevoir de l'information (compte) très utile, qui pouurait par exemple contribuer à la détection de transactions frauduleuses ou peut lui notifier certaines opérations de paiement refusées ou l'informer sur les frais de transactions transfrontalières.
Alors que que la Banque recommande l'acceptation de ces notifications, le client qui ne souhaite plus recevoir ces notifications, peut supprimer cette fonctionnalité lui-même via le menu 'plus/préférences', comme défini à l'article 4.4.1.2.

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, des limites standard (modifiables de façon limitée) sont appliquées aux ordres de virement via mobile banking (les virements instantanés, ordres de paiement permanants et ordres d'épargne automatique inclus):

6.1. Majeurs:

*Pour les majeurs, une limite journalière (0-24h) standard de 25.000 EUR est d'application par client.
Pour cette limite journalière les limites journalières maximales suivantes sont d'application :
- Pour des ordres de virement vers des bénéficiaires qui sont repris dans 'la liste des bénéficiaires' : 25.000 EUR
- Pour des ordres de virement vers des bénéficiaires qui ne sont pas repris dans 'la liste des bénéficiaires' : 5000 EUR.
Des virements entre des comptes dont le client est titulaire, co-titulaire ou mandataire ne sont pas comptés dans cette limite journalière.

*La limite de transaction par ordre de virement dépendra dans la pratique également de la limite journalière disponible d'application pour le client, mais une limite de transaction maximum absolue de 125.000 EUR par ordre de virement est le standard en vigueur, même si la limite journalière du client est plus élevée, et même s'il s'agit d'ordres de virement entre des comptes dont le client est titulaire, co-titulaire ou mandataire, où la limite journalière ne joue pas.

6.2. Mineurs d'âge (12-17 ans) :

* Pour les mineurs d'âge, une limite journalière (0-24h) standard de 250UR est d'application par client..
Dans cette limite journalière, les limites journalières maximales suivantes sont d'application :
- Pour des virements vers des bénéficiaires repris dans ' la liste des bénéficiaires' : 250 EUR par jour (0-24h) par client.
- Pour des ordres de virements vers des bénéficiaires non repris dans 'la liste des bénéficiaires' : 50 EUR.

Des virements entre des comptes dont le client est titulaire, co-titulaire ou mandataire ne sont pas comptés dans cette limite journalière.

*La limite de transaction par ordre de virement dépendra dans la pratique également de la limite journalière disponible d'application pour le client, mais une limite de transaction maximum absolue de 250EUR par ordre de virement est le standard en vigueur, même si la limite journalière du client est plus élevée, et même s'il s'agit d'ordres de virement entre des comptes dont le client est titulaire, co-titulaire ou mandataire, où la limite journalière ne joue pas.

6.3.Le client et le représentant légal peuvent à tout moment demander via l'agence du client de **modifier** (augmenter ou diminuer) les limites dans certaines limites.

La Banque se réserve le droit de refuser l'exécution de demandes qui sont incomplètes ou qui prêtent à confusion ou dont l'authenticité n'est pas sûre, comme défini dans le Règlement Général des Opérations.

6.4.Le cas échéant, par exemple parce que le montant (total) de (des) ordre(s) de virement introduit(s) par le client dépasse une certaine limite ou pour d'autres raisons de sécurité, il peut être demandé au client de signer les ordres de virement une deuxième fois via une des moyens de signature.

6.5.Lorsque le client ajoute un nouveau bénéficiaire à sa liste de bénéficiaires via mobile banking, les limites mentionnées ci-dessus pour les ordres de virement vers ce bénéficiaire repris dans 'la liste des bénéficiaires' ne seront d'application qu'après 24h.

6.6 Toutes les limites susmentionnées sont d'application par genre d'appareil(s) sur le(s)quel(s) le client a installé mobile banking (par exemple pour le(s) smartphone(s), pour la/les tablette(s), …).

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

6.8.Les limites d'application pour le client peuvent être consultées via Homebanking mais ne peuvent pas être adaptées via Homebanking.

Article 7: Imputation des transactions et opérations et preuve.

7.1. Connexion à mobile banking

L'utilisation simultanée de l'appareil sur lequel mobile banking est activé ainsi que un moyen d'accès et de signature pour lancer une session mobile banking selon les instructions du système, constitue la preuve de l'identité du client et de la validité de l'utilisation du moyen d'accès et de signature de mobile banking.

7.2. Ouverture ou demandes d'un compte, produit ou service

Chaque ouverture ou demande d'un nouveau compte, produit ou service, dont également la demande d'un prêt, signée à l'aide d'un des moyens d'accès et de signature, est réputée avoir été exécutée avec l'autorisation du client.

Le client reconnaît que ces moyens d'accès et de signature, pour l'application du présent règlement, constituent la signature du client.

Ceci vaut également pour la 2ème personne (non-demandeur) dont l'autorisation est requise pour l'ouverture d'un compte/produit.

7.3. Imputation des opérations de paiement/opérations d'investissement

Tout ordre de paiement qui, via mobile banking, vient à être encodé et signé à l'aide d'un,ou de plusieurs, si cela est jugé préférable pour des raisons de sécurité, des moyens d'accès et de signature, est réputée avoir été exécutée avec l'autorisation du client.

Les ordres de paiement qui sont correctement introduits et signés à l'aide des moyens d'accès et de signature sont 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.

Chaque enregistrement d'un bénéficiaire qui n'est pas encore enregistré (dans le cadre ou non d'un ordre de paiement que le client souhaite introduire à ce moment, qui est signé avec un ou, si cela est jugé préférable pour des raisons de sécurité, plusieurs des moyens d'accès et de signature, est censé avoir été introduit avec l'accord du client.

Toute transaction d'investissement sur un compte-titres, qui est introduite et confirmée à l'aide d'un des moyens d'accès et de signature, est réputée avoir été exécutée avec l'autorisation du client.

Le client reconnaît que les moyens d'accès et de signature constituent sa signature électronique, qui répond aux exigences légales en matière d'opposabilité et d'intégrité du contenu de l'ordre.

Le client reconnaît la validité juridique de toutes les transactions de paiement et d'investissement initiées via mobile banking et exécutées par la Banque, qui ont été signées avec les moyens d'accès et de signature.
La signature d'un ordre avec les moyens d'accès et de signature forme une preuve valable et suffisante de l'accord du client avec l'existence et le contenu de l'ordre.

7.4. Conservation et preuve des opérations de paiement et d'investissement

Toutes les données de chaque opération de paiement et d'investissement introduite et/ou exécutée par mobile banking sont enregistrées au moment de l'opération et conservées par la Banque pendant au moins dix 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.

7.5. Imputation d'autres actions

Toute transaction autre qu'une opération de paiement ou d'investissement, chaque action ou toute demande, signée ou non par voie électronique, effectuée ou encodée par mobile banking, comme défini dans cet article est réputée avoir été exécutée avec l'autorisation du client.
Le client reconnaît la validité juridique de ces opérations, actions et demandes initiées et signées ainsi et exécutées par la Banque

Article 8: Droits et obligations afférents au mobile banking

Sans préjudice des droits et obligations de la Banque et du client afférents à la carte de débit AXA et au homebanking, comme exposé dans les règlements applicables, les règles suivantes s'appliquent spécifiquement à 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 des comptes à vue et d'épargne d'une part et de bordereaux d'autre part, la Banque informe le client de toutes les opérations de paiement et d'investissement 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.

Pour les bordereaux concernant des transactions d'investissement, elle comporte notamment la dénomination du titre (à l'aide d'un code ISIN), le type d'ordre (ordre d'achat, de vente ou de souscription), la quantité, le prix unitaire, le montant de la transaction, la monnaie, la date valeur de l'inscription au débit ou au crédit et la date de l'exécution des transactions.

2°- La Banque empêchera toute nouvelle utilisation de mobile banking, pour autant que techniquement possible, dès l'instant où la notification de la perte, du vol ou de l'abus dont question à l'article 9 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 et de signature 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 ou de refuser temporairement (les ordrres pour l') exécution de certaines opérations de paiement ou d'investissement initiées via mobile banking et validées à l'aide des moyens d'accès et de signature, entre autres dans les cas suivants :
a) lorsque le compte est insuffisamment provisionné ; les ordres de paiement pour lesquels le compte n'est que partiellement approvisionné ne sont pas exécutés ;
b) lorsque l'ordre est incorrect, imprécis ou incomplet, ou ne répond pas à toutes les conditions d'application pour un certain type de transaction de paiement (e.a. virements instantanés).
c) lorsque certaines dispositions légales interdisent à la Banque d'exécuter l'ordre ;
d) lorsque le client a négligé de satisfaire à ses obligations vis-à-vis de la Banque ;
e) lorsque la Banque sait ou présume que le client n'a pas autorisé l'ordre ;
f) lorsque le client ne peut pas ou ne peut plus utiliser seul le compte – par exemple, parce qu'il a besoin de l'autorisation d'un autre titulaire du compte ou d'un représentant légal ;
g) lorsque le client a négligé de se conformer aux prescriptions et aux procédures en vigueur pour la communication d'ordres de paiement et d'investissement ;
h) lorsque l'ordre de paiement est donné dans une devise autre que l'euro ;
i) lorsque la Banque a connaissance de, ou présume une fraude, abus ou d'autres menaces en matière de sécurité ;
j) lorsque la Banque sait ou présume que l'ordre de paiement ou l'opération de paiement ou d'investissement qui en résulte, contrevient aux règles ou aux obligations auxquelles elle est soumise ;
k) lorsque la banque où le compte du bénéficiaire est ouvert ne fait pas partie du réseau de paiement de la Banque ou n'est pas joignable por un certain type de transaction de paiement (e.a. virements instantanés) ;
l) il est techniquement impossible pour la Banque de traiter l'opération d'une manière sécurisée
m) lorsqu'il est jugé utile pour la sécurité du système ou pour les intérêts financiers de la Banque ou du client
n) pour tout autre motif fondé dans le chef de la Banque.

Pour le refus de transactions d'investissement, il est référé en outre au Règlement des Services d'Investissement.

Lorsque la banque refuse d'exécuter une opération de paiement ou refuse d'initier une opération de paiement via mobile banking, elle met les informations relatives à ce refus à la disposition du client via mobile banking. Pour autant que possible et qu'elle y soit autorisée, elle mentionne également le motif du refus et les éventuelles modalités de correction si le refus d'exécution de l'ordre de paiement se fonde sur des erreurs matérielles. Si le refus est objectivement motivé, la Banque peut dès lors porter des frais en compte, tels que mentionnés dans la liste des tarifs.

Si la Banque ne refuse que temporairement un ordre de paiement via mobile banking, les délais d'exécution normaux pour l'exécution d'ordres de paiement via mobile banking, ne commencent qu'à courir au moment où la raison du blocage temporaire cesse d'exister.

5°- Outre le droit dont elle dispose de bloquer la carte de débit AXA comme prévu dans le Règlement carte de débit AXA, et de bloquer le homebanking comme prévu dans le Règlement homebanking, la Banque se réserve le droit de bloquer l'accès pour des raisons objectivement motivées relatives à la sécurité de mobile banking, à la présomption d'utilisation non autorisée ou frauduleuse de mobile banking, ou aux moyens d'accès et

de signature, et ce notamment dans les cas suivants:

- lorsqu'un code secret erroné a été saisi plusieurs fois de suite comme exposé à l'article 3;
-lorsque l'empreinte digitale du client a été refusée quelques 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.
- lorsque la Banque constate qu'elle ne dispose pas de certaines données légales du client

Lorsque la Banque procède à un tel blocage, elle en informe le client, si possible avant ou immédiatement après le blocage, oralement, par écrit ou par voie électronique, sauf si des considérations de sécurité objectivement motivées font obstacle à cette notification ou si elle est interdite au regard de la législation en vigueur.
La Banque débloquera l'accès à mobile banking dès que les raisons du blocage auront cessé d'exister.

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

7°- La Banque garantit au mieux de ses possibilités le bon fonctionnement et la continuité de mobile banking et des services afférents, et met à tout moment tout en œuvre pour assurer la sécurité des systèmes. 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 de logiciel; dans de telles circonstances, elle mettra tout en œuvre pour limiter ces interruptions à un minimum; les interruptions ne génèrent aucun droit à des dommages-intérêts pour le client.

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.

9°- Via mobile banking et son site Web, la Banque informera le client des mesures préventives à prendre pour éviter tout usage illicite de mobile banking.

La Banque informera le client en cas de soupçon de fraude ou de fraude avérée ou d'éventuelles menaces pour la sécurité.
Des notifications générales concernant des menaces pour la sécurité, se feront via le site web de la Banque ou via homebanking ou mobile banking après que le client se soit connecté.
Des notifications personnelles au client en cas de fraude avérée ou soupçon de fraude via mobile banking, se feront via un message personnel dans homebanking, ou par téléphone.

10°- La Banque s'attache en permanence à améliorer et étoffer le service mobile banking et sera dès lors régulièrement amenée à publier de nouvelles versions de mobile banking, dont le client sera informé en temps opportun.

8.2. Droits et obligations du client

1°-Le droit d'accès à et l'utilisation de l'application mobile banking, tout comme les moyens d'accès et de signature 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 de débit AXA doit prendre concernant la sécurité de celle-ci et la confidentialité du code pin et qui sont décrites dans le Règlement carte de débit 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 ses moyens d'accès et de signature à 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 communiquera jamais ses moyens d'accès et de signature à mobile banking par téléphone ou email ;

- il veillera à toujours encoder ses moyens d'accès et de signature dans la plus stricte discrétion ;

- en cas de modification de son code secret, il sélectionne un nouveau code 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 ;

- il donnera accès à un tiers l'à son appareil qu'après avoir complètement clôturé la session mobile banking; il ne mettra 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;

- il 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;

- aux divers stades de confirmation d'une transaction d'investissement, il vérifiera systématiquement si le titre, le nombre et le montant de la transaction correspond effectivement à la transaction d'investissement concernée.

- 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.

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 de débit 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 comme exposé 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.
Le client reconnaît que la Banque s'attache en permanence à améliorer et étoffer les services de mobile banking et sera donc régulièrement amenée à publier de nouvelles versions de mobile banking. Le client s'engage à procéder dans les meilleurs délais à la mise à jour de son application mobile banking et à toujours utiliser la version la plus récente de l'application.

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 irrévocablement et sans 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 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 d'exécution souhaitée dans le futur.

7°- Le client s'engage à veiller à ce que l'appareil qu'il utilise pour mobile banking réponde aux critères de sécurité requis. Il s'abstiendra à tout moment de débrancher intentionnellement les systèmes de sécurité.

Article 9: Perte, vol et utilisation abusive de mobile banking

9.1. Perte, vol et utilisation abusive d'un appareil

En cas de perte ou de vol d'un appareil sur lequel est installée une application de mobile banking ou en cas de présomption d'usage abusif de mobile banking quel qu'il soit, le client doit immédiatement faire bloquer l'application mobile banking sur l'appareil concerné. Le cas échéant, il est tenu de le faire pour chaque appareil séparément et pour chaque application 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 customer care de la Banque au numéro 03 286 66 55 et faire bloquer mobile banking,
Si le client est titulaire d'un compte à vue ou compte d'épargne, 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 blocage via CARDSTOP de la carte du client, n'implique pas automatiquement que l'application mobile banking, installée via cette carte sur un ou plusieurs appareils, est également bloquée.

Le client peut bien entendu réinstaller ensuite mobile banking sur un (autre) appareil, via l'enregistrement prévu à l'article 3.

9.2. Falsification, utilisation abusive ou non autorisée et perte ou vol des moyens d'accès et de signature

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 sur les appareils concernés 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, lors de notification de l'usage abusif de mobile banking à la banque suivant l'article 10, 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.

Article 10: Notification à la Banque d'opérations de paiement ou d'investissement non autorisées, non exécutées, mal ou tardivement 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 ou d'investissement non autorisée ou opération non correctement exécutée via mobile banking, dont il constate l'existence.

La notification d'opérations de paiement par mobile banking, initiées à partir d'un compte à vue ou autre compte dont le client prétend qu'elles n'étaient pas autorisées, n'ont pas été exécutées, ont été mal ou tardivement exécutées, doit se faire conformément aux dispositions et conditions de l'article 11 du Règlement comptes à vue.

La notification d'opérations d'investissement dont le client prétend qu'elles n'ont pas été autorisées ou été irrégulièrement exécutées, doit se faire conformément au Règlement services d'investissement.

10.2. Si le client est uniquement titulaire de comptes start2bank, il peut aussi notifier (les) opération(s) de paiement ou d'investissement non autorisée(s) ou non correctement exécutée(s) à la Banque, via homebanking.

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 10 du présent règlement, et les procédures d'introduction de contestations y exposées, les règles et dispositions exposées à l'article 12 du Règlement comptes à vue sont d'application pour les plaintes portant sur les services de paiement proposés par la Banque (dont mobile banking).

Article 12: Responsabilité d'opérations de paiement non autorisées, non exécutées, mal ou tardivement exécutées par mobile banking

12.1. Responsabilité d'opérations de paiement non autorisées par mobile banking

(1) En cas d'opération de paiement non autorisée par mobile banking, la Banque remboursera immédiatement le montant de l'opération non autorisée au client, et en tout état de cause au plus tard à la fin du premier jour bancaire ouvrable qui suit la notification de la transaction par le client à la Banque.
Le cas échéant, la Banque rétablira le compte (à vue) débité de ce montant dans la situation où il se serait trouvé si l'opération de paiement non autorisée n'avait pas eu lieu.
La date de valeur à laquelle le compte est crédité n'est pas postérieure à la date à laquelle il avait été débité du montant. La Banque remboursera également les autres éventuelles conséquences financières subies par le client, si ces dernières ont été correctement et raisonnablement établies.

Ce remboursement s'effectue toujours sous réserve. S'il appert après examen approfondi de la transaction contestée, que l'opération était bien autorisée ou que le client est responsable des pertes liées à la transaction non-autorisée, comme défini ci-après, la Banque peut de plein droit et sans mise en demeure débiter du compte du client le montant et tous les frais éventuels à la date valeur à laquelle le compte a été crédité, même s'il en résulte une situation de débit (non autorisée).

Si après enquête, la Banque est raisonnablement fondée à soupçonner une fraude dans le chef du client, elle ne procèdera pas au remboursement et en avertira les autorités nationales compétentes.

(2) Jusqu'à la date de la notification évoquée ci-dessus, le client reste responsable de toutes les conséquences de l'utilisation abusive de mobile banking.

Cette responsabilité est toutefois limitée à un montant de 50 euros pour le client qui agit en dehors du cadre de ses activités professionnelles ou d'entreprise.

Le client supporte toutes les pertes découlant d'opérations de paiement non autorisées qu'il a subies du fait qu'il a agi frauduleusement ou a omis, à dessein ou par négligence grave, d'utiliser mobile banking conformément aux conditions qui en régissent l'utilisation.

Sans préjudice des dispositions déjà évoquées ci-avant et dans d'autres règlements quant aux mesures préventives élémentaires visant la sécurité de mobile banking et des moyens d'accès et de signature, et toujours sous réserve de l'interprétation d'un juge qui tiendra compte de l'intégralité des circonstances matérielles, les manquements énumérés ci-dessous peuvent être assimilés à une négligence grave dans le chef du client:

- la consignation des moyens d'accès et de signature (code secret que le client a choisi) sous quelque forme que ce soit, sur un document conservé avec l'appareil, ou l'enregistrement du code secret dans l'appareil, sur un PC ou autre support.
- Omettre de notifier sans délai la perte, le vol ou l'utilisation abusive de l'appareil et/ou des moyens d'accès et de signature (cette notification ne peut souffrir aucun retard).
- L'opportunité offerte à un tiers, quel qu'il soit, de prendre connaissance du code secret et/ou d'utiliser une application de mobile banking qu'il a activée sur un appareil.
- Omettre de notifier sans retard à la Banque toute présomption ou constat d'une quelconque utilisation abusive.
- Omettre de notifier sans retard à la Banque la passation, telle que constatée sur les relevés bancaires ou extraits de compte, de toute opération effectuée en mobile banking qui n'a pas été autorisée ou qui aurait été mal exécutée.
- Omettre de notifier sans délai à la banque toute erreur ou irrégularité constatée sur les relevés bancaires ou extraits de compte.
- Abandonner l'appareil sur lequel l'application mobile banking est activée dans un véhicule ou lieu accessible au public, sauf s'il se trouve dans un tiroir ou armoire fermé à clef. Sont assimilés à des lieux accessibles au public, les sites auxquels un grand nombre de personnes ont effectivement accès, sans qu'il s'agisse nécessairement de lieux publics.
- Refuser de déposer plainte sans délai auprès des services de police, ou refuser de transmettre sans délai

à la Banque une copie du procès-verbal d'une plainte ainsi déposée.
- Faire un usage de mobile banking qui va à l'encontre des conditions contractuelles d'émission et d'utilisation.
-Utiliser les moyens d'accès et de signature pour mobile banking d'une façon contraire aux dispositions relatives à son utilisation
- S'abstenir de (faire) bloquer mobile banking lorsque la Banque en fait la demande.
- S'abstenir de (faire) bloquer mobile banking lorsque le client perçoit des signaux indiquant qu'un tiers peut accéder, a accès ou tente d'avoir accès à son appareil, au service mobile banking, à certaines de ses fonctionnalités et/ou à sa (ses) connexion(s) internet ou de télécommunication.
- La mise à disposition ou communication des moyens d'accès et de signature à des tiers quels qu'ils soient.
- Abandonner son appareil, pour quelque motif que ce soit, pendant une session mobile banking ouverte, même pour une très courte période.

(3) Par dérogation au point précédent, le client, qui agit en dehors de ses activités professionnels et d'entreprise, n'encourt aucune perte si:
* le détournement de mobile banking n'a pas pu être constaté par le client avant qu'un paiement ne soit effectué, sauf si le client a agi frauduleusement, ou
* la perte est due à des actes ou à une carence d'un employé, agent ou succursale de la Banque ou d'une entité vers laquelle les activités de la Banque ont été externalisées.
* le paiement par mobile banking a eu lieu sans recours à une authentification forte du client.

(4) Dès que le client a bloqué (fait bloquer) mobile banking, la responsabilité du client quant aux conséquences du détournement de mobile banking prend fin, sauf si la Banque apporte la preuve d'un agissement frauduleux dans le chef du client.
C'est le cas notamment quand il appert que, en dépit de la notification, le client continue à utiliser mobile banking lui-même, sous quelque forme que ce soit.
Toute nouvelle utilisation de mobile banking après notification sera rendue impossible pour autant que cela soit techniquement possible.

12.2. Responsabilité de la non-exécution, mauvaise exécution ou exécution tardive d'opérations de paiement par mobile banking

La Banque est responsable de l'exécution correcte et dans les délais de toutes les opérations de paiement par mobile banking qui ont été valablement et réglementairement initiées par le client, pour autant que le client ait rigoureusement respecté les conditions et modalités d'utilisation de mobile banking.

Pour ce qui concerne la responsabilité des opérations de paiement non exécutées, mal ou tardivement exécutées par homebanking, nous renvoyons aux dispositions en la matière exposées dans le Règlement comptes à vue.

12.3 Responsabilité en cas d'identifiant unique inexact

Un ordre de paiement effectuée par mobile banking conformément à l'identifiant unique est réputé dûment exécuté pour ce qui concerne le bénéficiaire indiqué par cet identifiant unique.

Pour les dispositions en matière de responsabilité, il est renvoyé au Règlement comptes à vue.

12.4. La Banque remboursera, si elle est responsable d'opérations de paiement non-autorisées ou incorrectement exécutées via mobile banking, également les éventuelles conséquences financières qui en découlent, notamment le montant des frais supportés par le client afin de déterminer le dommage à récupérer, pour autant que le client est en mesure de prouver le lien de causalité entre ces conséquences et frais et l'opération de paiement concernée.

Ce règlement est exclusivement d'application lorsque 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 la transaction concernée.

12.5. La responsabilité de la Banque n'est pas engagée lorsqu'une opération de paiement ou d'investissement initiée via mobile banking n'est pas exécutée ou n'est pas correctement exécutée pour cause de force majeure ou de 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 et nucléaires, défauts techniques graves ou autres catastrophes, désorganisation passagère des services postaux ou grève de la poste, mesures prises par des autorités nationales ou internationales, le non-respect par des tiers de leurs obligations à l'égard de la Banque pour des raisons indépendantes de leur volonté.

12.6. La Banque ne peut être tenue pour responsable des conséquences négatives éventuellement subies par le payeur ou le bénéficiaire du fait que la Banque est fermée à d'autres jours que les jours bancaires non ouvrables (qui peuvent être d'autres jours que les samedis, dimanches, jours fériés légaux ou de remplacement) ce qui rend l'exécution immédiate de transactions via mobile banking impossible. Le client est tenu de s'informer concernant de tels jours de fermeture.

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

12.8. 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 erreurs dus au fournisseur de l'appareil ou à n'importe quel tiers qui interviendrait dans la transmission ou la communication.

La Banque ne peut être mise en cause si le client a volontairement débranché des sécurités système de l'appareil sur lequel il utilise mobile banking.

12.9. La Banque ne peut être tenue pour responsable du préjudice quel qu'il soit qui découlerait de l'utilisation de mobile banking à des fins autres que les services décrits dans le présent règlement.

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

14.1 Le traitement des données à caractère personnel dans le cadre de mobile banking est conforme au Règlement général sur la protection des données (RGPD – GDPR), comme stipulé à l'article 1.9. du Règlement Général des Opérations.

14.2. Sans préjudice des dispositions du RGPD et de l'article 1.9. du Règlement Général des Opérations (informations fournies au client sur le traitement des données à caractère personnel par la Banque et les droits du client dans ce cadre), la Banque assure, en tant que prestataire de services de paiement, le traitement des données à caractère personnel nécessaire en vue de l'exécution de la convention passée avec le client concernant mobile banking, ou nécessaire et pertinent en vue de la prévention, la recherche et la détection d'escroquerie au paiement et en vue d'en éviter toute utilisation abusive.

La Banque a uniquement accès aux données à caractère personnel requises pour la prestation de services de paiement, dont mobile banking, et ne peut les traiter et stocker que moyennant autorisation expresse du client préalablement à l'exécution des opérations de paiement.
Le client donne cette autorisation expresse en approuvant l'exécution de l'opération de paiement, comme exposé à l'article 3.

Les clients qui, dans le cadre de l'utilisation de mobile banking, communiquent à la Banque les données de (d'autres) personnes physiques, par exemple de payeurs ou bénéficiaires d'opérations de paiement effectuées via mobile banking, y sont autorisés uniquement si les personnes concernées en ont été préalablement et suffisamment informées, et y ont consenti. La Banque décline toute responsabilité à cet égard.
Le client accepte que ses données à caractère personnel et celles d'autres personnes physiques puissent être communiquées dans le cadre de l'exécution d'ordres de paiement par homebanking, soit au payeur ou au bénéficiaire, soit à des tiers que le client y a expressément autorisés.

14.3. Lors de l'utilisation de mobile banking par le client, 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 et du fonctionnement de ce service et pour pouvoir résoudre des problèmes. 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 de débit AXA, du lecteur de carte et de certaines opérations conformément à la liste des tarifs en vigueur 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.

La Banque se réserve également le droit, sans respecter ce délai de préavis et sans notification préalable, de mettre sans délai fin au droit d'utilisation de mobile banking, si le client ne s'est pas connecté à mobile banking pendant une période de 18 mois à la suite.

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 périodiques afférents à mobile banking sont dus au pro rata seulement par le client jusqu'à la fin de la convention.
Les frais afférents à 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.

Le client peut accepter ou rejeter les modifications annoncées pendant ce délai de 2 mois.

A défaut d'une notification dans les 2 mois que le client n'accepte pas les modifications, il est réputé avoir accepté les modifications qui lui seront immédiatement opposables.

Si le client n'accepte pas les modifications annoncées, il peut décider, dans ce délai de deux mois, de résilier le service mobile banking sans frais et avec effet immédiat, et en informer la Banque, auquel cas le droit d'utiliser mobile banking dans son chef et/ou pour son compte, prend irrémédiablement fin.

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. Ceci peut s'effectuer par exemple via la page 'Nouvelles' que le client voit dès qu'il s'est connecté dans mobile banking.
Le client est réputé souscrire aux nouvelles dispositions dès qu'il utilise la fonctionnalité ou le service concerné.