Authentification Non Rejouable
ANR D'accès à Crédit Coopératif Direct
(Sécurisation des Opérations en Ligne - SOL)

Conditions Générales d'Utilisation
(Avenant au contrat Crédit Coopératif Direct figurant dans les conditions générales de la Convention de Compte de Dépôt)

Les présentes Conditions Générales d'Utilisation du « service Authentification Non Rejouable - ANR » constituent un des éléments contractuels du service Crédit Coopératif Direct dont les dispositions figurent dans la Convention de Compte de Dépôt. Elles annulent et remplacent les conditions générales d'utilisation du service Authentification renforcée précisées à l'art. 8.6.5 de la convention de compte de dépôt.

Ces conditions générales n'ont pas pour objet ou effet de modifier en quoi que ce soit le contenu du contrat porteur « Carte Bancaire » signé par le client avec la Banque à l'occasion de la remise de sa carte. Les dispositions du contrat porteur continuent donc de s'appliquer au client dans toutes ses dispositions, même si les mêmes moyens d'ANR dédiés au porteur sont mis en œuvre dans le cadre de la sécurisation de transaction de paiement E-conmmerce

1- Le service Authentification Non Rejouable

1.1- Description du service Authentification Non Rejouable

Le service Authentification Non rejouable ANR, ci après dénommé « le service », est un service de la Banque de renforcement de la sécurité qui permet aux clients qui ont souscrit au « service » de réaliser certaines opérations sensibles telles que précisées à l'art. 1.2, dans le cadre de Crédit Coopératif Internet, et protégées par un système d'Authentification Non Rejouable. La liste de ces opérations est disponible sur le portail de la Banque.

Il est réservé aux clients de la Banque abonnés au service « Crédit Coopératif Direct ».

Dans le cadre du « Service :

- soit : la Banque envoie un code de contrôle par SMS vers le numéro de téléphone mobile de l'abonné au « service ». Ce code de contrôle doit être saisi par l'abonné au « Service » afin de réaliser les opérations sensibles.

- soit : l'abonné calcule un code de contrôle au moyen de sa Carte Bancaire et d'un lecteur d'authentification (lecteur CAP) Ce code de contrôle doit être saisi par l'abonné au « service » afin de réaliser les opérations sensibles.

1.1.1 - Utilisation du code de contrôle

L'utilisation du code de contrôle est d'usage unique, aléatoire et temporairement limité dans le temps lors de la session Web sur Crédit Coopératif Internet. Ce code de contrôle propre à l'Authentification Non rejouable est distinct et complémentaire du mot de Passe lorsqu'il est demandé aux abonnés à Crédit Coopératif Direct lors des connexions à Crédit Coopératif Internet.

1.1.2 - Utilisation du lecteur d'authentification

Lors de la validation d'une opération concernée par le renforcement de sécurité, il sera demandé au Client de saisir un code de contrôle sur huit chiffres, unique et non réutilisable.

Ce code de contrôle sera communiqué au Client via le lecteur d'authentification associé à la carte bancaire du Client après saisie sur le lecteur du code confidentiel de la dite carte et, éventuellement, des informations liées à cette dernière.

Le nombre d'essais successifs de composition sur le lecteur d'authentification du code confidentiel est limité à 3 (trois), avec conformément, à l'article 16.4.1 de la convention de compte « Carte Bancaire », le risque d'invalidation de la carte au 3éme essai infructueux.

Le lecteur d'authentification peut être utilisé selon 3 (trois) modes :

- le mode 'mot de passe unique' : qui délivre un code de contrôle sur 8 (huit) chiffres, unique et non réutilisable après saisie, par le Client, du code confidentiel de sa carte,

- le mode 'défi/réponse' : qui délivre un code de contrôle sur 8 (huit) chiffres, unique et non réutilisable après saisie, par le Client, du code confidentiel de sa carte et d'une donnée liée à l'opération ou non,

- le mode 'signature' : qui délivre un code de contrôle sur 8 (huit) chiffres, unique et non réutilisable après saisie, par le Client, du code confidentiel de sa carte et d'une ou plusieurs données liées à l'opération.

Il est de la responsabilité du Client de vérifier la validité des données qu'il saisit sur le lecteur d'authentification.

Le recours au lecteur d'authentification est assimilé (mode signature), aux termes de l'article 1316-4 du Code civil, à une signature électronique laquelle "consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle se rattache".

1.1.3 - Durée – Restitution - du lecteur

Le lecteur est attribué au client pour une durée indéterminée.

Le lecteur pourra être restitué à tout moment par le client mais par cette restitution, ce dernier accepte de ne plus avoir accès aux opérations nécessitant la sécurité renforcée non rejouable.

Par ailleurs, la Banque se réserve le droit de bloquer la validation d'opérations par le biais du lecteur, sans préavis, en cas d'utilisation frauduleuse par le client du lecteur d'authentification.

L'utilisation de ce lecteur étant liée à la détention par le client d'une carte bancaire émise par la Banque, la résiliation, l'annulation ou bien encore, la fin de validité de la ou des cartes du client pour quelque cause que ce soit, entraînera l'interruption immédiate et de plein droit de l'utilisation du lecteur pour les opérations de paiement effectuées au moyen d'une carte bancaire.

1.1.4 - Propriété du lecteur

Le lecteur reste, en tout état de cause, la propriété de la Banque. Il est donc incessible et intransmissible à quelque titre et pour quelque cause que ce soit. Le Client ne pourra en aucune façon apporter une quelconque modification au lecteur qui lui a été remis. Toute modification non-autorisée du lecteur par le Client, se fera sous sa responsabilité et entraînera la suspension immédiate du service. La Banque ne pourra en aucune façon voir sa responsabilité engagée à raison des éventuelles conséquences dommageables d'une telle modification.

1.1.5 - Perte ou vol du lecteur

Le Client est responsable du lecteur qui lui a été remis. En cas de perte ou de vol du lecteur, le Client a l'obligation de prévenir la Banque.

La Banque ne saurait être tenue pour responsable vis-à-vis du client en cas de perte ou de vol du lecteur, non plus que des conséquences liées à cette perte ou ce vol.

1.2 - Description des opérations sensibles réalisées par l'intermédiaire de Crédit Coopératif Internet protégées par un système d'Authentification Non Rejouable dans le cadre du « Service »

Ces opérations sensibles sont fixées comme suit :

- La création de RIB en vue d'enregistrer un nouveau compte externe parmi ceux déjà inscrits par l'abonné à Crédit Coopératif Internet afin d'effectuer un virement vers le compte externe d'un bénéficiaire non enregistré au préalable dans l'abonnement à Crédit Coopératif Internet

1.3 - Transmission du code de Contrôle par SMS

La Banque ne peut être tenue pour responsable d'une anomalie lors de l'acheminement du SMS transmis due à:

- Un dysfonctionnement du réseau employé ou des systèmes du client (ordinateur ou téléphone défaillant) et ce, quelle que soit la cause de l'anomalie d'acheminement,
- Une erreur de manipulation du fait du client (numéro de téléphone erroné, mémoire du téléphone mobile…) ou,
- Un fait constitutif d'un cas de force majeure (interruption du réseau...).

Pour recevoir le message SMS contenant le code de contrôle, vous devez respecter la zone de couverture de votre opérateur téléphonique.

En cas de non-respect de ces conditions, la Banque ne peut être tenue responsable des incidents de réception des messages SMS.

Dans le cas de réception de messages, nous attirons votre attention sur le fait que les informations qui circulent sur les réseaux de communication ne sont pas cryptées et que le bon acheminement, la confidentialité ou l'intégrité de ces informations ne peuvent être garantis.

Il vous appartient de prendre toutes les précautions nécessaires afin que l'accès aux communications arrivant sur votre téléphone portable ne puisse se faire que de manière sécurisée, notamment après saisie d'un mot de passe, afin d'éviter une consultation par des tiers non autorisés. En tout état de cause, vous demeurez seul responsable :

- De votre choix d'opérateur de téléphonie,
- Des paramétrages de votre téléphone mobile,
- Des précautions qui vous incombent de préserver la confidentialité des accès à votre téléphone mobile.

Les communications par voie électronique pouvant être porteuses de virus informatiques au travers des programmes téléchargés, il vous appartient de choisir la/les solution(s) de protection qui lui semblera(ont) la/les plus appropriée(s). Vous vous engagez à prévenir, sans délai, la Banque de tout événement rendant impossible l'accès au « service » (notamment, changement d'opérateur, perte ou vol de votre téléphone mobile, changement de numéro de téléphone etc…).
En cas de défaut d'information de votre Banque, vous ne pourrez présenter aucune réclamation de quelque nature que ce soit liée à cet incident.

1.4 - Souscription au service Authentification Non rejouable - Modalités

Les présentes conditions générales d'utilisation du « service » constituent un des éléments contractuels de votre contrat Crédit Coopératif Direct, qui est à disposition dans votre Centre d'Affaires ou sur le site www.credit-cooperatif.coop de votre Banque et qui font partie intégrante de votre convention de compte de dépôt. En cas de souscription au « service » vous acceptez les présentes conditions générales d'utilisation du « service » sans préjudice des dispositions contractuelles de votre contrat Crédit Coopératif Direct.

Le service Authentification Non Rejouable peut être souscrit en ligne sur Crédit Coopératif Internet ou bien dans un Centre d'Affaires de la Banque.

Toute souscription au service Authentification Non Rejouable est subordonnée à la détention ou à l'ouverture par vous ou par votre représentant légal, d'un compte dans les livres de la Banque.
En cas de compte joint, chaque cotitulaire du compte peut utiliser le service. Dans ce cas, chaque cotitulaire doit souscrire individuellement au service Authentification Non Rejouable.

S'agissant d'un client mineur, la souscription à ce service devra être effectuée par son(ses) représentant(s) légal(aux).

1.5 - Tarification du service Authentification Non Rejouable

La souscription au service d'Authentification Non Rejouable est gratuite.

1.6 – Durée- Résiliation. - Modification du service

Le service Authentification Non Rejouable est conclu, pour une durée indéterminée. Le contrat prend effet à l'acceptation en ligne des conditions générales d'utilisation du « service » ou à la signature en Centre d'Affaires des conditions générales de vente.

La Banque se réserve le droit de modifier les modalités du service après en avoir préalablement informé le client. La modification aura lieu sans préavis si elle est rendue nécessaire, notamment, par de nouvelles obligations de nature légale, la mise en place de solutions techniques nouvelles afin de renforcer la sécurité du service

Le client peut modifier à sa convenance les modalités d'adressage du code de contrôle par SMS, soit via son Centre d'Affaires, soit par courrier auprès de son conseiller clientèle. La Banque prendra en compte ces modifications et lui fera parvenir une confirmation par écrit (envoi de courrier électronique ou papier).

Par ailleurs, le service peut être résilié à tout moment à votre initiative par lettre recommandée avec accusé de réception adressée au Centre d'Affaires qui gère le compte. Cette résiliation prend effet à compter de la date de réception de la lettre de résiliation par la
Banque.
Le service peut être résilié par la Banque à tout moment. Cette résiliation prend effet le mois suivant la date d'envoi de la lettre de résiliation.

1.7 - Responsabilité de l'abonné au « Service »

Les dispositifs de sécurité mis en place par la Banque ne dégagent pas la responsabilité du client qui se doit :

- Sous sa responsabilité, de protéger son matériel informatique avec la solution de sécurité (pare-feu et anti-virus notamment) de son choix et de maintenir ces dispositifs à jour en permanence
- De toujours vérifier que les données des opérations qu'il souhaite valider (Nom, coordonnées bancaire des bénéficiaires, ...) n'ont pas été altérées.
- De ne jamais divulguer ses codes confidentiels (le code confidentiel de sa carte en particulier). Aucun collaborateur de la Banque ou un intermédiaire ne peut le lui demander.
- De ne pas répondre à des sollicitations de tiers qui tenteraient de se faire passer pour la Banque à travers des emails, loteries, prétendus dysfonctionnements ou vérifications diverses pour demander au client ses identifiants, mot de passe, code confidentiel ou code généré par les nouvelles solutions de sécurité.

1.8 - Convention de preuve

Le Client et la Banque conviennent que les opérations effectuées avec validation d'un code généré par le lecteur seront réputées avoir été effectuées par le Client, sauf pour lui à rapporter la preuve contraire.

1.9 - Informations contractuelles par courrier électronique

Le client accepte expressément que la Banque, s'agissant du service objet des présentes, puisse lui adresser, par courriers électroniques, des informations relatives aux présentes et à leur exécution.