

## Règlement myCrelan

### Définitions

Dans le cadre du présent Règlement, les termes repris ci-dessous ont la signification définie ci-après :

a. « **Banque** » : fait référence à Crelan en tant que Fédération d'établissements de crédit visée par l'article 240 de la loi du 25 avril 2014 relative au statut et au contrôle des établissements de crédit. La Banque est composée des sociétés de droit belge ci-après dont le siège est situé boulevard Sylvain Dupuis, 251 à 1070 Bruxelles:  
- SA Crelan, TVA-BE 0205.764.318 – RPM Bruxelles;  
- SCRL CrelanCo, TVA-BE 0403.263.840 – RPM Bruxelles.

Ces sociétés sont reprises dans la liste des établissements de crédit agréés en Belgique tenue par la Banque Nationale de Belgique (BNB) située Boulevard du Berlaimont 14 à 1000 Bruxelles (site internet: [www.bnb.be](http://www.bnb.be)), qui constitue l'autorité de contrôle prudentielle.

La Banque exerce ses activités, entre autres, au travers d'un réseau d'agences dont les coordonnées (adresse, numéros de téléphone, heures d'ouverture) sont disponibles sur le site internet [www.crelan.be](http://www.crelan.be).

b. « **myCrelan** » : service de banque par Internet de Crelan qui permet au Titulaire de l'accès, d'accéder en ligne aux Comptes Liés du Client pour y exécuter des opérations bancaires. L'accès à myCrelan peut être demandé par l'intermédiaire d'une agence.

c. « **Client(s)** » : personne(s) physique(s) ou morale(s), (co-)titulaire(s) du ou des Compte(s) Lié(s) au(x)quel(s) le Titulaire de l'accès se voit octroyer la possibilité d'accéder aux comptes concernés par myCrelan.

d. « **Titulaire de l'accès** » : personne physique à qui la Banque délivre les Moyens d'accès au(x) Compte(s) Lié(s) par myCrelan. Le Titulaire est obligatoirement le Client ou son mandataire, ou le représentant du Client. Le Titulaire agit au nom et pour compte du Client.

e. « **Compte(s) Lié(s)** » : comptes du Client ouverts auprès de la Banque sur lesquels sont imputées les opérations effectuées avec les Moyens d'accès du Titulaire de l'accès par myCrelan. Un ordre ne peut être exécuté que s'il y a une provision suffisante sur le Compte Lié et si le compte concerné autorise ce type d'ordre.

f. « **Limite** » : montant maximum qui peut être débité des Comptes Liés par type de transaction ou par période, en fonction du Client considéré. Cette Limite englobe les opérations effectuées au moyen de toutes les applications digitales mises à

disposition par Crelan (par exemple myCrelan, Crelan Mobile, Crelan Tablet, ...). La Limite standard est communiquée sur support durable. Le Client qui le souhaite peut demander en agence ou par myCrelan une adaptation des Limites standards fixées. Le Client doit faire attention sur le fait qu'il existe aussi des limites spécifiques par application digitale (Crelan Mobile, Crelan Tablet, ...).

g. « **Provision** » : montant disponible sur le Compte Lié concerné à la date de l'opération considérée.

h. « **Moyens d'accès** » : le code d'utilisateur du Titulaire pour l'accès à myCrelan, le Digipass remis par la Banque au Titulaire de l'accès, le numéro de série du Digipass inscrit au dos de celui-ci, le code de 6 chiffres, unique et temporaire généré par le Digipass, le code secret de quatre chiffres choisi par le Titulaire de l'accès pour sécuriser son accès myCrelan et le code secret de quatre chiffres fourni par la Banque pour le premier accès. Tous ces moyens sont nécessaires et suffisants pour accéder, avec un ordinateur ou tout autre appareil, aux Comptes Liés par myCrelan.

i. « **Digipass** » : petit appareil qui permet de générer des codes de 6 chiffres temporaires pour l'accès aux Comptes Liés par myCrelan avec un ordinateur, une tablette ou tout autre appareil, d'y effectuer des opérations et de les signer électroniquement.

j. « **Crelan Mobile** » : application qui permet au Titulaire de l'accès, détenteur d'un smartphone, d'avoir un accès mobile aux Comptes Liés pour y exécuter certaines transactions.

k. « **Crelan Sign** » : application intégrée à Crelan Mobile qui permet au Titulaire de l'accès d'accéder à myCrelan et d'y signer des opérations bancaires.

l. « **Consommateur** » : toute personne physique qui agit à des fins qui n'entrent pas dans le cadre de son activité commerciale, industrielle, artisanale ou libérale.

-----

### 1. Champ d'application - Entrée en vigueur

Ce Règlement régit l'accès et l'utilisation de myCrelan. Il détermine les droits et devoirs du Client, de la Banque et du Titulaire de l'accès. Il entre en vigueur le 1<sup>er</sup> décembre 2018 et remplace à partir de cette date l'édition précédente datée du 20 novembre 2017.

Le Règlement myCrelan est remis sur support durable lors de la demande d'accès à myCrelan.

Il est également disponible sur le premier écran du site internet myCrelan qui offre la possibilité de le télécharger et de l'imprimer.

Il est également possible d'en obtenir gratuitement un exemplaire en agence.

Le Client et le Titulaire de l'accès adhèrent au Règlement myCrelan lors de la signature de la demande d'accès myCrelan. Chaque utilisation confirme leur adhésion.

La Banque assure également un support pratique par l'intermédiaire de son service desk qui est joignable pendant les heures d'ouverture du service par courriel: [mycrelan@crelan.be](mailto:mycrelan@crelan.be) ou par téléphone: (0032) (0)2.558.78.88.

## **2. Application du Règlement général des opérations bancaires**

Ce règlement est un complément au Règlement général des opérations bancaires de Crelan qui est intégralement applicable dans la mesure où il n'y est pas dérogé par les présentes dispositions. En cas de contradiction, les dispositions du présent Règlement priment.

Le Client a reçu un exemplaire du Règlement général des opérations bancaires au début de sa relation avec Crelan et peut toujours en obtenir un nouvel exemplaire dans son agence et sur [www.crelan.be](http://www.crelan.be).

Lorsque le Client utilise Crelan Sign, le Règlement Crelan Mobile et Crelan Tablet est aussi applicable.

## **3. Accès à myCrelan**

L'accès à myCrelan est uniquement octroyé sur demande du Client adressée à la Banque. Il est individuel et strictement personnel au Titulaire de l'accès. Les Moyens d'accès sont délivrés par voies séparées au Titulaire de l'accès et Crelan supporte le risque de leur envoi éventuel. Crelan peut refuser la délivrance des Moyens d'accès sans devoir se justifier.

Moyennant restitution du Digipass défectueux, le Titulaire de l'accès peut en recevoir gratuitement un nouveau.

A défaut d'une adresse d'envoi spécifiquement mentionnée dans la demande, les Moyens d'accès sont envoyés à la dernière adresse principale du Titulaire de l'accès communiquée à la Banque.

Les Moyens d'accès sont strictement personnels et réservés aux personnes physiques. Le Client-personne morale, doit communiquer les références d'une personne physique de son choix, appelée le Titulaire de l'accès, qui utilisera myCrelan au nom et pour compte du Client et qui exercera en pratique tous les droits et obligations qui découlent du présent Règlement.

La première connexion et l'activation de l'accès à myCrelan se fait avec le code délivré à ce effet par la Banque. Il faut ensuite choisir un code secret personnel sur base de la procédure qui est jointe lors de l'envoi du Digipass. Après avoir effectué le choix d'un code secret personnel, le code délivré par la Banque peut être détruit.

Le Client qui a déjà un accès actif à Crelan Online ne doit plus faire de nouvelle activation pour accéder à myCrelan.

Pour pouvoir accéder par la suite aux Comptes Liés et y effectuer des opérations avec myCrelan, un code de 6 chiffres secret, temporaire et à usage unique, doit être encodé sur le clavier de l'ordinateur chaque fois que le système myCrelan l'exige. Ce code de 6 chiffres à usage unique doit chaque fois être généré au moyen du Digipass et du code secret personnel du Titulaire de l'accès. Sur base de l'encodage du code de 6 chiffres en vigueur au moment considéré, le système reconnaît le Titulaire de l'accès et les opérations effectuées par myCrelan exécutées par imputation sur le Compte Lié concerné.

Les Titulaires qui ont un accès actif à Crelan Mobile peuvent par ailleurs également obtenir un accès à myCrelan et y faire des opérations bancaires en fasant usage de Crelan Sign. Si le Titulaire choisi de se signaler par Crelan Sign, myCrelan génère un code QR unique et sécurisé. Le Titulaire de l'accès ouvre Crelan Sign sur la page de connexion de Crelan Mobile, scanne le code QR et confirme avec son code secret personnel.

Les opérations effectuées avec myCrelan sont enregistrées par le système dans un journal électronique et dans les fichiers informatisés de la Banque.

## **4. Disponibilité de myCrelan**

La Banque garantit au mieux de ses capacités la continuité de myCrelan. Pour préserver la sécurité et la fiabilité de myCrelan, la Banque veille à ce que ses programmes et systèmes soient performants et dépourvus de virus.

La Banque peut interrompre myCrelan provisoirement pour l'entretien de ses programmes ou l'installation de nouvelles versions de software.

La Banque décline toute responsabilité en cas d'indisponibilité temporaire de myCrelan pour cause d'entretien annoncé, d'entretien inopiné d'une durée raisonnable ou de circonstances imprévues ne relevant pas du contrôle immédiat de la Banque. Ces interruptions n'octroient au client aucun droit à une indemnité.

## **5. Durée – suspension - fin**

Celui qui a obtenu un accès aux Comptes Liés par myCrelan conserve le droit de disposer de cet accès aussi longtemps que celui-ci n'a pas été résilié et qu'il subsiste au moins un Compte à vue Lié ouvert auprès de la Banque. Le Client et le Titulaire de l'accès peuvent renoncer à tout moment et gratuitement à myCrelan. Dans ce cas, le Digipass doit être remis à la Banque.

Il est toujours possible de bloquer l'accès myCrelan aux Comptes Liés en introduisant cinq fois successivement un code de 6 chiffres incorrects lors de la connexion.

Le blocage immédiat de l'accès peut aussi être obtenu sur simple demande par téléphone au numéro (0032) (0)2.558.78.88. La demande doit être ensuite confirmée par courrier adressé dans les trois jours ouvrables à Crelan – Service BOPa Electronic Banking - Boulevard Sylvain Dupuis 251 à

1070 Bruxelles, par fax au numéro (0032) (0)2.558.76.30. ou par courriel à l'adresse [bopa.ElectronicBanking@crelan.be](mailto:bopa.ElectronicBanking@crelan.be).

La Banque peut bloquer, suspendre ou supprimer le droit d'utiliser myCrelan à n'importe quel moment avec un préavis de deux mois adressé par écrit selon le cas, au Client ou au Titulaire de l'accès.

La Banque peut bloquer l'accès sans préavis pour des raisons ayant trait à la sécurité, à la possibilité d'une utilisation non autorisée ou frauduleuse de myCrelan, ou sur injonction des autorités. A titre d'exemple, la Banque peut bloquer l'accès dans les cas suivants : apparition d'anomalie(s), problème(s) technique(s) ou indices de piratage informatique ou de tentative de piratage mettant en cause la sécurité de myCrelan, possible(s) manquement(s) aux consignes de sécurité, indices d'abus ou de tentative d'abus de la confiance de la Banque, de celle du Client ou de celle du Titulaire de l'accès.

La Banque informe le Client et/ou le Titulaire de l'accès de sa motivation par lettre, extrait de compte (ou annexe), message dans myCrelan, courriel, fax, SMS ou tout autre moyen qui apparaît le plus approprié et sécurisé eu égard au cas concret et à la situation personnelle du Client, si possible de manière préalable ou au plus tard immédiatement après le blocage, sauf si des raisons objectives de sécurité, un ordre de justice ou une loi l'interdisent. La Banque débloque l'accès et délivre gratuitement de nouveaux Moyens d'accès dès la disparition de la raison ayant nécessité le blocage.

Le blocage de l'accès empêche toute nouvelle opération par myCrelan, mais les opérations déjà encodées et validées avant le blocage seront exécutées normalement.

En cas de fraude, le Titulaire de l'accès doit prévenir la banque dans les plus brefs délais afin de procéder au blocage des Comptes Liés.

## 6. Services liés à myCrelan

Les opérations énumérées ci-dessous sont réalisables par myCrelan :

**a. Virements électroniques en euros** entre les différents Comptes Liés auxquels le Titulaire de l'accès a accès sans application des limites périodiques et virements par le débit du Compte à vue Lié vers un compte de tiers, même ouvert dans une autre banque, avec application des limites périodiques.

**b. Paiements instantanés**. L'expression "paiement instantané", fait référence à un paiement électronique individuel pouvant être effectué 24 heures sur 24 et 7 jours sur 7 (24/7/365) entre banques qui participent à ce système grâce auquel les fonds sont mis à la disposition du bénéficiaire en quelques secondes. La possibilité de faire des paiements instantanés par myCrelan est prévue pour fin novembre 2018.

**c. Consultation du solde des Comptes Liés**, d'un historique des dernières opérations effectuées, de la liste des domiciliations et des ordres permanents en

cours, d'un relevé des dépenses par carte de crédit, des crédits accordés ou autres avoirs détenus par le Client auprès de la banque.

**d. Création, annulation, modification d'ordres permanents en euros**. Les ordres permanents de virement peuvent être passés en ligne sur base des périodicités suivantes : tous les mois, deux mois, trois mois, quatre mois, six ou douze mois. Le montant, la communication et la date de fin d'un ordre permanent sont modifiables. Ces ordres peuvent être annulés immédiatement ou à une date future sans préjudice de paiements déjà effectués par le système.

**d. Annulation d'un ordre de débit de domiciliations**. La révocation d'une domiciliation avec myCrelan a un effet immédiat et pour l'avenir. A certaines conditions, un paiement réalisé sur base d'une domiciliation est révocable rétroactivement. Il y a lieu de se référer au Règlement des Opérations pour connaître ces conditions.

**f. Utilisation du service optionnel Zoomit**. Le Client qui a opté pour des documents électroniques comme entre autres des factures et des fiches de salaire provenant de différents fournisseurs, peut les consulter via Zoomit. Si un ordre de paiement est lié au document électronique, Zoomit facilite l'exécution des paiements en complétant les données de base de l'ordre à l'aide des données de la facture. Le contenu des documents livrés appartient à la relation contractuelle entre le Client et ses fournisseurs. La Banque n'est pas responsable du contenu et de l'exactitude des documents électroniques.

**f. Gestion des limites** : le Client peut gérer les limites de ses applications digitales auprès de Crelan (myCrelan, Crelan Mobile, Crelan Tablet, ...).

**h. Demande de prêt à tempérament**. Via un lien placé dans myCrelan, il est possible d'introduire électroniquement une demande de prêt à tempérament.

MyCrelan est en constante amélioration. D'autres fonctionnalités peuvent être développées. La Banque en informe le Client et le Titulaire de l'accès par les moyens appropriés.

## 7. Tarifification et frais

La délivrance du Digipass, son maintien à disposition, son remplacement et l'usage de myCrelan peuvent impliquer des frais qui seront débités du Compte Lié ou d'un autre compte du Client. Celui-ci se référera à la tarification reprise dans les listes de tarifs de Crelan disponibles gratuitement en agence et sur le site web de la banque : [www.crelan.be](http://www.crelan.be).

En cas de résiliation, les frais annuels payés à l'avance sont remboursés sans délai au prorata de la période restant à courir à dater du premier jour du mois suivant la date de la résiliation.

## **8. Modification du contrat**

La Banque a le droit de modifier le présent Règlement ou les frais comptés dans le cadre de myCrelan à tout moment moyennant information du Client au moins deux mois avant que la modification ne sorte ses effets. Les modifications des taux d'intérêts ou de change entrent en application immédiatement lorsqu'elles se font sur base d'un taux ou cours de référence convenu.

Le Client est réputé avoir accepté toute modification à défaut pour lui d'avoir notifié son refus par écrit à la Banque avant la date d'entrée en vigueur prévue. Ce refus est gratuit et équivaut à une renonciation immédiate à myCrelan. Dans ce cas, le Digipass doit être restitué à la Banque.

## **9. Authentification du Titulaire de l'accès et signature des ordres**

Le système qui supporte myCrelan reconnaît le Titulaire de l'accès, ouvre l'accès au(x) Compte(s) Lié(s) et aux fichiers de la Banque et exécute les ordres encodés dans l'ordinateur (ou tout autre appareil permettant la connexion à myCrelan) lorsque les Moyens d'accès ont été correctement utilisés. Sur base de l'encodage du code de 6 chiffres généré par le Digipass, le système reconnaît le Titulaire de l'accès et les opérations effectuées par myCrelan sont donc authentifiées et exécutées par imputation sur le Compte Lié concerné. Ces opérations sont aussi enregistrées par le système dans un journal électronique et dans les fichiers informatisés de la Banque.

Le Titulaire de l'accès reconnaît que le code de 6 chiffres créé avec le code secret du Titulaire, constitue une signature électronique qui a la même force probante qu'une signature manuscrite et répond à l'article 1322 alinéa 2 du Code Civil. L'introduction de ce code prouve que le Titulaire de l'accès marque son accord sur l'exécution de l'opération.

Le Titulaire de l'accès qui utilise Crelan Sign pour signer des opérations, reconnaît que l'introduction du code secret personnel dans Crelan Mobile forme une signature électronique qui a la même force probante qu'une signature manuscrite et répond à l'article 1322 alinéa 2 du Code Civil. L'introduction de ce code prouve que le Titulaire de l'accès marque son accord sur l'exécution de l'opération effectuée par myCrelan.

## **10. Risques - Avertissement**

Tout manquement aux consignes de sécurité génère un risque important d'utilisation abusive ou frauduleuse de myCrelan au détriment du Client, du Titulaire de l'accès ou de la Banque. Le système exécute les opérations encodées et les impute sur les Comptes Liés sans vérifier l'identité réelle de la personne qui s'est connectée avec les Moyens d'Accès personnels du Titulaire de l'accès. Toute personne, éventuellement malhonnête qui dispose de ces Moyens d'Accès est en mesure d'utiliser myCrelan pour passer des opérations sur les Comptes Liés (consultations, paiements, virements électroniques, etc.). Par conséquent, il est

indispensable que le Titulaire et le Client respectent scrupuleusement les consignes de sécurité.

## **11. Consignes de sécurité**

Le Titulaire de l'accès doit conserver les Moyens d'accès et les utiliser dans des conditions de sécurité optimales, sous un contrôle permanent et exclusif, afin que personne d'autre que lui ne puisse les utiliser ou en utiliser une contrefaçon pour accéder électroniquement aux Comptes Liés.

Les Moyens d'accès sont strictement personnels au Titulaire de l'accès, ce qui signifie que seul celui-ci est autorisé à en avoir connaissance ou à les utiliser. Le Titulaire de l'accès a l'interdiction de confier les Moyens d'accès à des tiers, même s'il s'agit de proches.

Le Titulaire de l'accès doit prendre les précautions nécessaires à la préservation de la confidentialité de ses différents codes clés. Il doit particulièrement veiller à la confidentialité de son code secret (Pin), le mémoriser immédiatement, détruire tout support le reprenant, ne jamais le retranscrire, ne jamais les révéler à d'autres personnes même s'il s'agit de proches du Client ou de personnes prétendant agir au nom de la Banque. Lors du choix de son code secret, le Titulaire de l'accès doit éviter les combinaisons trop faciles à découvrir (par exemple une date de naissance, 1234, 1111, etc.). Il doit protéger son code secret des regards indiscrets lorsqu'il l'encode dans le Digipass. Chaque fois que la confidentialité de son code secret est menacée, le Titulaire de l'accès doit le modifier immédiatement en introduisant l'ancien code secret dans le Digipass, puis en maintenant enfoncée la touche ◀ pendant quelques secondes et en introduisant ensuite son nouveau code secret et en l'encodant une deuxième fois pour confirmation.

Le Titulaire de l'accès doit accorder le même degré de prudence à la préservation du code secret de 6 chiffres unique et temporaire généré par le Digipass aussi longtemps que l'accès myCrelan ouvert avec ce code de 6 chiffres n'est pas clôturé. Il doit également conserver le Digipass sous son contrôle exclusif.

### **Attention**

Crelan ne demandera jamais de communiquer par courriel, par téléphone ou de quelque manière que ce soit des données personnelles telles qu'un code secret, un numéro de compte, un numéro de série de Digipass, ...). Si le Titulaire de l'accès reçoit ce genre de correspondance, il est supposé savoir que l'émetteur de celle-ci n'est pas la Banque mais qu'il s'agit de courriels, d'appels, ... frauduleux auxquels le Titulaire de l'accès ne doit pas et ne peut pas répondre. Si le Titulaire de l'accès y donne suite, la fraude lui sera imputée et il n'y aura pas de dédommagement. Les e-mails malveillants doivent être signalés à la banque par courriel à l'adresse phishing@crelan.be.

Le Titulaire de l'accès s'engage à veiller à ce que son ordinateur, sa tablette ou tout autre appareil permettant l'accès à myCrelan réponde aux exigences de sécurité habituelles dans le domaine

informatique et aux utilisateurs de l'internet, comme par exemple disposer d'un système d'exploitation qui est à jour, disposer d'un anti-malware (anti-virus, anti-spam,...) performant, ne pas avoir des logiciels pirates, ... .

Lorsqu'il se connecte au site myCrelan, le Titulaire de l'accès doit faire attention aux faux sites internet qui pourraient imiter le site de Crelan. La connexion à myCrelan doit en particulier se faire de manière directe par le site de la Banque. Il est par exemple strictement interdit de se connecter en cliquant sur un lien reçu : la Banque n'envoie jamais de message avec un lien permettant de se connecter à myCrelan, que ce soit par mail, whatsapp, SMS, messenger, ou par tout autre moyen de communication.

Ces mesures sont aussi d'application lorsque le Client accède au site de Crelan pour confirmer qu'il a donné son autorisation à un tiers prestataire de services de paiement d'accéder à ses comptes dans le cadre de services d'initiation de paiement ou de services d'information sur les comptes. Dans une telle situation, le Client doit également faire attention à se connecter au véritable site de ce tiers prestataire de services de paiement.

Le Titulaire de l'accès s'engage également à ne jamais laisser sans surveillance son ordinateur ou ses appareils permettant l'accès à myCrelan, ainsi qu'à ne pas les transmettre à un tiers avec une session myCrelan ouverte.

Le Titulaire de l'accès doit également veiller à ce que la session se déroule toujours dans un environnement sécurisé.

En cas de vol, de perte du Digipass, de contrefaçon, d'accès non autorisé aux Comptes Liés ou toute autre anomalie laissant supposer un abus ou un risque d'abus de l'accès myCrelan aux Comptes Liés, le Titulaire de l'accès doit immédiatement contacter la Banque pour bloquer l'accès myCrelan.

Le blocage immédiat de l'accès s'obtient aussi avec cinq introductions successives d'un code secret temporaire de six chiffres incorrect ou sur simple demande par téléphone au numéro (0032) (0)2.558.78.88.

La Banque peut enregistrer les appels téléphoniques pour prévenir les contestations. Sur demande adressée à la Banque dans les 18 mois, le Titulaire de l'accès et le Client peuvent obtenir la preuve du blocage ou de la demande de blocage. La demande de blocage doit être confirmée par courrier adressé dans les trois jours ouvrables à Crelan - Service BOPa Electronic Banking, Boulevard Sylvain Dupuis 251 à 1070 Bruxelles ou par fax au numéro (0032) (0)2.558.76.30 ou par courriel à l'adresse [bopa.ElectronicBanking@crelan.be](mailto:bopa.ElectronicBanking@crelan.be).

Le Titulaire de l'accès doit aussi sans délai adresser à la Banque une relation écrite de l'incident et déposer une plainte auprès de la police (à l'étranger, auprès des autorités compétentes équivalentes). Une copie de la plainte ainsi que les références du dossier doivent être communiquées à la Banque. Le Client et le Titulaire doivent collaborer de leur mieux à l'enquête.

Tout manquement aux consignes de sécurité reprises ci-dessus constitue une négligence grave, de même que le fait pour le Client ou le Titulaire de noter ses données de sécurité personnalisées,

comme son numéro d'identification personnel ou tout autre code, sous une forme aisément reconnaissable, et notamment sur l'instrument de paiement ou sur un objet ou un document conservé ou emporté par le Client ou le Titulaire avec l'instrument de paiement, ainsi que le fait de ne pas avoir notifié au prestataire de services de paiement ou à l'entité indiquée par celui-ci, la perte ou le vol, dès qu'il en a eu connaissance.

Toute négligence grave, manquement intentionnel aux obligations prévues par le présent Règlement et toute fraude engage solidairement et indivisiblement le Titulaire de l'accès et le Client à l'égard de la Banque.

## **12. Mesures de sécurité prises par la Banque**

La Banque prend au sein de son organisation et de son réseau toutes mesures raisonnables de prudence. Elle assure au sein de son organisation la confidentialité du code secret délivré au Titulaire de l'accès en vue de sa première connexion et délivre ce code secret séparément du Digipass.

La Banque maintient la possibilité de bloquer l'accès myCrelan à disposition du Titulaire de l'accès pour lui permettre de bloquer immédiatement l'accès par internet aux Comptes Liés en cas de risque d'abus.

La Banque se réserve le droit de bloquer d'initiative cet accès en cas de menace sur la sécurité du service myCrelan ou en cas de risque d'utilisation non autorisée ou frauduleuse de ce service. Sauf si la loi, une injonction judiciaire ou des autorités ou des raisons de sécurité s'y opposent, elle en informe le Titulaire de l'accès ou le Client, si possible de manière préalable et au plus tard immédiatement après le blocage.

## **13. Responsabilités – opérations non-autorisées ou incorrectement réalisées**

La Banque est responsable à l'égard du payeur de la bonne exécution des ordres électroniques correctement initiés qui lui parviennent correctement. Il convient de se référer au Règlement général des opérations bancaires pour toutes précisions sur les réclamations, responsabilités, opérations de paiement non autorisées ou incorrectement réalisées et sur le droit éventuel à une indemnisation.

Ci-dessous sont reprises des règles spécifiques aux opérations sur Compte Lié réalisées au moyen d'un instrument de paiement.

Lorsque la sécurité des Moyens d'accès aux Comptes Liés n'a pas été préservée (code d'utilisateur du Titulaire de l'accès, Digipass, numéro de série du Digipass, code de 6 chiffres unique et temporaire généré par le Digipass, code secret de quatre chiffres choisi par le Titulaire pour sécuriser son accès myCrelan et le code secret de quatre chiffres donné par la banque pour le premier accès), c'est le Client qui assume les pertes liées à toute opération de paiement non autorisée jusqu'à ce que la Banque en ait été avertie ou que le blocage ait été demandé



par téléphone au numéro (0032) (0)2.558.78.88 ou par courriel à [bopa.ElectronicBanking@crelan.be](mailto:bopa.ElectronicBanking@crelan.be).

Le risque à charge du Client payeur qui a la qualité de consommateur est toutefois limité à un montant de 50 EUR. Par dérogation à ceci, le Client payeur consommateur ne supporte aucune perte si :

1° la perte, le vol ou le détournement de l'instrument de paiement ne pouvait être détecté par le payeur avant le paiement, sauf s'il a agi frauduleusement, ou

2° la perte est due à des actes ou à une carence d'un salarié, d'un agent ou d'une succursale de la Banque ou d'une entité vers laquelle ses activités ont été externalisées.

Le Client payeur supporte toutes les pertes occasionnées par des opérations de paiement non autorisées si ces pertes résultent soit d'un agissement frauduleux de sa part, soit du fait qu'il n'a pas satisfait, intentionnellement ou à la suite d'une négligence grave, à une ou plusieurs des obligations qui lui incombent, dont notamment les consignes de sécurité mentionnées plus haut.

Lorsque la Banque n'exige pas une authentification forte de son Client payeur, celui-ci ne supporte aucune perte financière éventuelle, à moins qu'il n'ait agi frauduleusement.

En cas de vol, perte ou détournement des Moyens d'accès, la Banque supporte intégralement la perte résultant d'opérations non autorisées réalisées après la demande de blocage de l'accès auprès du numéro de téléphone (0032)(0)2.558.78.88 ou par courriel à [bopa.ElectronicBanking@crelan.be](mailto:bopa.ElectronicBanking@crelan.be), sauf en cas de fraude du Client, du Titulaire de l'accès ou de leur mandataire qui dans cette hypothèse n'ont aucun recours contre la Banque, laquelle peut engager leur responsabilité solidairement et indivisiblement pour la récupération de son dommage éventuel.

Le Titulaire de l'accès doit aussi sans délai adresser à la Banque une relation écrite de l'incident et déposer une plainte auprès de la police (à l'étranger, auprès des autorités compétentes équivalentes). Une copie de la plainte ainsi que les références du dossier doivent être communiquées à la Banque. Le Client et le Titulaire doivent collaborer de leur mieux à l'enquête.

#### **14. Preuve**

Un journal électronique de la Banque enregistre les données pertinentes des opérations réalisées par myCrelan avec les Moyens d'accès du Titulaire de l'accès. En cas de contestation, la Banque peut reproduire le contenu de l'enregistrement sur support papier ou sur tout autre support. Sans préjudice du droit du Client et du Titulaire de l'accès d'apporter la preuve contraire par tous les moyens, il est convenu que l'enregistrement correct d'opérations analogues avant et après l'opération en cause constitue une preuve du fait que le système a fonctionné correctement et que l'opération en cause n'a pas été affectée par une déficience technique ou autre. Les données enregistrées dans le journal électronique de la Banque peuvent être opposés au titre de preuve au Client non Consommateur, sans préjudice de son droit d'apporter la preuve contraire. L'enregistrement d'une opération réalisée par

myCrelan avec les Moyens d'accès correspondant au Compte concerné permet de présumer jusqu'à preuve du contraire, que le Client ou le Titulaire de l'accès a lui-même initialisé et approuvé (signé électroniquement) l'opération.

Des extraits de compte communiqués ou mis à disposition ainsi que prévu au Règlement général des opérations bancaires et dans les conventions particulières, reprennent en détail les frais comptés par Crelan ainsi que les opérations réalisées sur le Compte par myCrelan.

#### **15. Correspondance**

Le Client qui a un accès à myCrelan, reçoit de manière standard sa correspondance pour tous ses comptes par voie électronique. Dans ce cas les extraits de compte et les annexes ne sont pas envoyés par la poste.

Le Client qui souhaite recevoir ses extraits de compte par la poste peut le demander dans son agence ou par myCrelan.

MyCrelan offre également la possibilité d'imprimer ses extraits de compte.

Le Client s'engage à prendre connaissance des communications à caractère non commercial émanant de la Banque au moins une fois tous les quinze jours.

#### **16. Réclamations – plaintes - litiges**

Les réclamations peuvent être introduites conformément à ce qui est prévu dans le Règlement général des opérations bancaires.

Les actions et litiges concernant les services visés par le présent Règlement sont de la compétence exclusive des juridictions belges. Le droit belge est applicable.

#### **17. Tiers intervenants**

Les interruptions, perturbations, dysfonctionnements trouvant leur origine hors de la Banque, notamment ceux qui engagent d'autres opérateurs (les perturbations du réseau internet, d'électricité etc.) ou qui mettent en cause un matériel non agréé (ordinateur personnel, tablette ou tout autre appareil permettant l'accès à myCrelan) par la Banque n'engagent pas sa responsabilité.

La Banque est étrangère aux contrats de vente de l'ordinateur utilisé pour passer des ordres bancaires ainsi qu'aux contrats passés par le Client ou le Titulaire de l'accès avec d'autres opérateurs (internet, électricité, vendeurs des services ou produits payés avec myCrelan etc.). Le Client et le Titulaire de l'accès se référeront donc à ces opérateurs pour connaître leurs conditions contractuelles, notamment de responsabilité et de tarif.

#### **18. Droit d'usage et propriété**

La Banque est propriétaire des programmes, applications et documentation relatifs à myCrelan. Le contrat avec le Client n'entraîne aucun transfert de propriété en matière de droits intellectuels ou de procédés.

Le Titulaire de l'accès dispose seulement d'un droit d'usage strictement personnel de myCrelan. Il ne peut en disposer autrement que dans le cadre des utilisations prévues dans le Règlement. Il ne peut autoriser des tiers à en disposer de quelque manière que ce soit.

Le Client n'est pas autorisé à mettre à disposition de tiers, de travailler, reproduire ou modifier de quelque manière que ce soit les marques, logos, programmes de logiciels, documentation ou tout autre élément de myCrelan, gratuitement ou moyennant rémunération, partielle ou totale sans un accord écrit préalable de la Banque. Le Digipass délivré par la Banque reste sa propriété exclusive et doit lui être restituée lorsqu'il est mis fin à son utilisation.

### **19. Utilisation de photographies dans myCrelan**

Le Client peut personnaliser myCrelan en ajoutant une photo personnelle. Le Client s'engage à n'utiliser aucune photo qui serait en contravention avec les dispositions légales ou les droits de tiers, dont les droits de propriété intellectuelle tels que les droits d'auteurs, les droits de dessins et de modèles. La Banque se réserve le droit de refuser ou de retirer toute photo qui contreviendrait à ces règles.

### **20. Langue**

La relation entre le Client, le Titulaire de l'accès et la Banque s'établit dans la langue de la région dans laquelle le Client demande la délivrance de l'accès myCrelan ou sur base de la langue convenue par les parties.

---