COMMISSION
EUROPÉENNE

Bruxelles, le 3.8.2022
C(2022) 5517 final

**RÈGLEMENT DÉLÉGUÉ (UE) …/... DE LA COMMISSION**

**du 3.8.2022**

**modifiant les normes techniques de réglementation définies dans le règlement délégué (UE) 2018/389 en ce qui concerne la dérogation de 90 jours pour l'accès aux comptes**

(Texte présentant de l'intérêt pour l'EEE)

# EXPOSÉ DES MOTIFS

## 1. CONTEXTE DE L'ACTE DÉLÉGUÉ

L'Autorité bancaire européenne (ABE) a été chargée, en vertu de l'article 98, paragraphe 1, de la directive (UE) 2015/2366 (directive sur les services de paiement ou DSP2), d'élaborer des projets de normes techniques de réglementation relatives à l'authentification forte du client et à des normes ouvertes communes et sécurisées de communication (ci-après «normes techniques de réglementation SCA&CSC»). Ces normes techniques de réglementation devaient préciser un certain nombre d'exigences, notamment en ce qui concerne l'authentification forte du client et les dérogations à l'application de celle-ci. Les normes techniques de réglementation SCA&CSC qui ont alors été élaborées par l'ABE ont été adoptées par la Commission le 27 novembre 2017 et publiées au Journal officiel de l'Union européenne sous la forme du règlement délégué (UE) 2018/389 de la Commission, qui est applicable depuis le 14 septembre 2019.

En vertu de l'article 98, paragraphe 5, de la DSP2, l'ABE est tenue de régulièrement réexaminer et, le cas échéant, actualiser les normes techniques de réglementation, afin notamment de tenir compte de l'innovation et des évolutions technologiques. La Commission est habilitée à adopter des normes techniques de réglementation conformément aux articles 10 à 14 du règlement (UE) nº 1093/2010 instituant l'ABE, tel que modifié par le règlement (UE) 2019/2175. Conformément à l'article 10, paragraphe 1, du règlement (UE) nº 1093/2010, la Commission doit statuer sur l'adoption des projets de norme dans les trois mois suivant leur réception. Elle peut aussi n'adopter ceux-ci que partiellement, ou moyennant des modifications, lorsque l'intérêt de l'Union l'exige.

## 2. CONSULTATION AVANT L'ADOPTION DE L'ACTE

Conformément à l'article 10, paragraphe 1, du règlement (UE) nº 1093/2010, l'ABE a mené une consultation publique sur les projets de normes techniques de réglementation modificatives soumis à la Commission. Elle a publié un document de consultation sur son site web le 28 octobre 2021, et la consultation s'est achevée le 25 novembre 2021. L'ABE a sollicité l'avis du groupe des parties intéressées au secteur bancaire visé à l'article 37 du règlement (UE) nº 1093/2010 sur les projets de normes techniques de réglementation modificatives et a présenté un document expliquant comment le résultat des consultations avait été pris en compte dans la version finale de ces projets soumise à la Commission.

Conformément à l'article 10, paragraphe 1, du règlement (UE) nº 1093/2010, l'ABE a également présenté à la Commission son analyse d'impact, comprenant une analyse des coûts et avantages, pour la version finale des projets de normes techniques de réglementation modificatives. Cette analyse peut être consultée à l'adresse suivante: https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/regulatory-technical-standards-on-strong-customer-authentication-and-secure-communication-under-psd2 (pages 20 à 24 du rapport final sur les projets de normes techniques de réglementation modificatives).

## 3. ÉLÉMENTS JURIDIQUES DE L'ACTE DÉLÉGUÉ

La version finale des projets de normes techniques de réglementation modificatives introduit dans le règlement délégué (UE) 2018/389 de la Commission une nouvelle dérogation obligatoire à l'obligation d'authentification forte du client. En vertu de cette dérogation, lorsque les clients passent par un prestataire de services d'information sur les comptes pour

accéder aux informations concernant leurs comptes de paiement, les prestataires gestionnaires de comptes sont tenus de ne pas appliquer l'authentification forte si certaines conditions destinées à garantir la sûreté et la sécurité des données de l'utilisateur de services de paiement sont remplies. Il faut notamment que l'étendue des données soit limitée, que le prestataire de services de paiement gestionnaire de comptes applique l'authentification forte du client lors du premier accès et la renouvelle périodiquement, et qu'il puisse à tout moment décider d'appliquer l'authentification forte s'il a des raisons objectivement motivées et documentées de le faire liées à un accès non autorisé ou frauduleux. Les projets de normes techniques de réglementation modificatives restreignent, parallèlement, le champ d'application de la dérogation volontaire prévue à l'article 10 du règlement délégué (UE) 2018/389 de la Commission en la limitant aux seuls cas où le client accède directement aux informations relatives au compte. En outre, les projets de normes techniques de réglementation modificatives font passer de 90 jours à 180 jours le délai à l'échéance duquel l'authentification forte doit être renouvelée lorsque les dérogations susmentionnées s'appliquent. Les prestataires de services de paiement gestionnaires de comptes qui offrent à la fois une interface dédiée et un mécanisme d'urgence ne sont pas tenus de mettre en œuvre la dérogation à l'authentification forte du client dans le cadre du mécanisme d'urgence, pour autant qu'ils n'appliquent pas la dérogation à l'authentification forte du client dans leurs canaux clients directs.

**RÈGLEMENT DÉLÉGUÉ (UE) …/... DE LA COMMISSION**

**du 3.8.2022**

**modifiant les normes techniques de réglementation définies dans le règlement délégué (UE) 2018/389 en ce qui concerne la dérogation de 90 jours pour l'accès aux comptes**

(Texte présentant de l'intérêt pour l'EEE)

LA COMMISSION EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne,

vu la directive (UE) 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur, modifiant les directives 2002/65/CE, 2009/110/CE et 2013/36/UE et le règlement (UE) nº 1093/2010, et abrogeant la directive 2007/64/CE[1], et notamment son article 98, paragraphe 4, deuxième alinéa,

considérant ce qui suit:

(1) L'article 10 du règlement délégué (UE) 2018/389 de la Commission[2] prévoit qu'il peut être dérogé à l'obligation d'authentification forte du client prévue à l'article 97 de la directive (UE) 2015/2366 lorsqu'un utilisateur de services de paiement accède au solde et aux opérations récentes d'un compte de paiement sans que des données de paiement sensibles soient divulguées. Dans ce cas, les prestataires de services de paiement sont autorisés à ne pas appliquer l'authentification forte du client pour l'accès aux informations relatives au compte, à condition qu'elle ait été appliquée la première fois qu'il a été accédé aux informations sur le compte et au moins tous les 90 jours par la suite.

(2) Le recours à cette dérogation a conduit à une grande divergence des pratiques dans le cadre de l'application du règlement délégué (UE) 2018/389, certains prestataires de services de paiement gestionnaires de comptes exigeant une authentification forte du client tous les 90 jours, d'autres à intervalles plus courts, et d'autres encore n'ayant pas appliqué la dérogation et exigeant une authentification forte du client lors de chaque accès au compte. Cette divergence a engendré des frictions indésirables dans le parcours client lors de l'utilisation des services d'information sur les comptes et a eu une incidence négative sur les services des prestataires de services d'information sur les comptes.

(3) Afin de concilier les différents objectifs de la directive (UE) 2015/2366, à savoir améliorer la sécurité, faciliter l'innovation et renforcer la concurrence dans le marché intérieur, il est nécessaire de préciser davantage l'application de la dérogation prévue à l'article 10 du règlement délégué (UE) 2018/389 dans les cas où les informations relatives aux comptes sont consultées par l'intermédiaire d'un prestataire de services

[1] JO L 337 du 23.12.2015, p. 35.

[2] Règlement délégué (EU) 2018/389 de la Commission du 27 novembre 2017 complétant la directive (UE) 2015/2366 du Parlement européen et du Conseil par des normes techniques de réglementation relatives à l'authentification forte du client et à des normes ouvertes communes et sécurisées de communication (JO L 69 du 13.3.2018, p. 23).

d’information sur les comptes. En conséquence, dans un tel cas, les prestataires de services de paiement ne devraient pas avoir la possibilité de choisir d’appliquer ou non l’authentification forte du client, et la dérogation devrait être rendue obligatoire, sous réserve que les conditions visant à garantir la sûreté et la sécurité des données des utilisateurs de services de paiement soient remplies.

(4) La dérogation devrait être limitée à l’accès au solde et aux opérations récentes d’un compte de paiement sans divulgation de données de paiement sensibles. La dérogation ne devrait s’appliquer que lorsque l’authentification forte du client a déjà été appliquée par les prestataires de services de paiement lors du premier accès par l’intermédiaire du prestataire de services d’information sur les comptes concerné et doit être renouvelée périodiquement.

(5) Afin de garantir la sûreté et la sécurité des données des utilisateurs de services de paiement, les prestataires de services de paiement devraient pouvoir à tout moment appliquer l’authentification forte du client lorsqu'ils ont des raisons objectivement motivées et documentées de le faire liées à un accès non autorisé ou frauduleux. Cela peut être le cas lorsque les mécanismes de contrôle des opérations mis en place par le prestataire de services de paiement gestionnaire du compte détectent un risque élevé d’accès non autorisé ou frauduleux. Afin de garantir une application cohérente de la dérogation, les prestataires de services de paiement gestionnaires de comptes devraient, dans de tels cas, documenter et dûment motiver auprès de leur autorité nationale compétente, à la demande de cette dernière, les raisons de l’application de l’authentification forte du client.

(6) Lorsque l’utilisateur de services de paiement accède directement aux informations relatives au compte, les prestataires de services de paiement devraient continuer d'avoir la possibilité de choisir d’appliquer ou non une authentification forte du client. En effet, aucun problème particulier nécessitant une modification de la dérogation prévue à l’article 10 du règlement délégué (UE) 2018/389 n’a été observé dans ce cas, contrairement au cas de l’accès par l’intermédiaire d’un prestataire de services d’information sur les comptes.

(7) Afin de garantir une concurrence équitable entre tous les prestataires de services de paiement, et conformément à l’objectif de la directive (UE) 2015/2366 de permettre le développement de services innovants et faciles à utiliser, il est proportionné de fixer le même délai de 180 jours pour le renouvellement de l’authentification forte du client, que ce soit pour l'accès aux informations relatives au compte directement auprès du prestataire de services de paiement gestionnaire du compte ou pour l’accès par l’intermédiaire d’un prestataire de services d’information sur les comptes. Le renouvellement de l’authentification forte du client à la fréquence actuelle pourrait engendrer des frictions indésirables dans le parcours client et empêcher les prestataires de services d’information sur les comptes d’offrir leurs services et les utilisateurs d’en bénéficier.

(8) Les prestataires de services de paiement gestionnaires de comptes qui proposent une interface dédiée et qui ont mis en place un mécanisme d’urgence conformément à l’article 33, paragraphe 4, du règlement délégué (UE) 2018/389 ne devraient pas être tenus de mettre en œuvre la nouvelle dérogation obligatoire dans leurs interfaces clients directes aux fins du mécanisme d’urgence, pour autant qu’ils n’appliquent pas la dérogation prévue à l’article 10 du règlement délégué (UE) 2018/389 dans leurs interfaces clients directes. Il serait disproportionné d’exiger des prestataires de services de paiement gestionnaires de comptes qui proposent une interface dédiée dans laquelle

ils doivent appliquer la nouvelle dérogation obligatoire qu'ils appliquent également la dérogation dans leurs interfaces clients directes aux fins du mécanisme d'urgence.

(9) Afin d'accorder aux prestataires de services de paiement suffisamment de temps pour apporter les modifications nécessaires à leurs systèmes, les prestataires de services de paiement gestionnaires de comptes devraient mettre à la disposition des prestataires de services de paiement les modifications apportées aux spécifications techniques de leurs interfaces pour se conformer au présent règlement, au moins 2 mois avant la mise en œuvre de ces modifications.

(10) Il convient de modifier en conséquence le règlement délégué (UE) 2018/389.

(11) Le présent règlement se fonde sur les projets de normes techniques de réglementation soumis à la Commission par l'Autorité bancaire européenne.

(12) L'Autorité bancaire européenne a procédé à des consultations publiques ouvertes sur les projets de normes techniques de réglementation sur lesquels se fonde le présent règlement, analysé les coûts et avantages potentiels qu'ils impliquent et sollicité l'avis du groupe des parties intéressées au secteur bancaire institué par l'article 37 du règlement (UE) nº 1093/2010 du Parlement européen et du Conseil[3].

(13) Le Contrôleur européen de la protection des données a été consulté conformément à l'article 42, paragraphe 1, du règlement (UE) 2018/1725 et a rendu un commentaire formel le 7 juin 2022.

(14) Afin de faciliter la transition vers les nouvelles exigences énoncées dans le présent règlement, il convient que les prestataires de services de paiement qui appliquaient la dérogation prévue à l'article 10 du règlement délégué (UE) 2018/389 avant l'entrée en application du présent règlement soient autorisés à continuer d'appliquer cette dérogation jusqu'à 90 jours à compter de la dernière fois que l'authentification forte du client a été appliquée,

A ADOPTÉ LE PRÉSENT RÈGLEMENT:

*Article premier*
***Modifications du règlement délégué (UE) 2018/389***

Le règlement délégué (UE) 2018/389 est modifié comme suit:

(1) L'article 10 est remplacé par le texte suivant:

[3] Règlement (UE) nº 1093/2010 du Parlement européen et du Conseil du 24 novembre 2010 instituant une Autorité européenne de surveillance (Autorité bancaire européenne), modifiant la décision nº 716/2009/CE et abrogeant la décision 2009/78/CE de la Commission (JO L 331 du 15.12.2010, p. 12).

*«Article 10*

*Accès aux informations sur le compte de paiement directement auprès du prestataire de services de paiement gestionnaire du compte*

1. Les prestataires de services de paiement sont autorisés à ne pas appliquer l'authentification forte du client, sous réserve du respect des exigences définies à l'article 2, lorsqu'un utilisateur de services de paiement accède en ligne à son compte de paiement directement, à condition que cet accès soit limité à l'un des éléments suivants en ligne sans que des données de paiement sensibles soient divulguées:

   (a) le solde d'un ou de plusieurs comptes de paiement désignés;

   (b) les opérations de paiement exécutées durant les 90 derniers jours par l'intermédiaire d'un ou de plusieurs comptes de paiement désignés.

2. Par dérogation au paragraphe 1, les prestataires de services de paiement ne sont pas exemptés de l'application de l'authentification forte du client lorsque l'une des conditions suivantes est remplie:

   (a) l'utilisateur de services de paiement accède en ligne aux informations visées au paragraphe 1 pour la première fois;

   (b) plus de 180 jours se sont écoulés depuis la dernière fois que l'utilisateur de services de paiement a accédé en ligne aux informations visées au paragraphe 1 et que la procédure d'authentification forte du client a été appliquée.».

(2) L'article 10 *bis* suivant est inséré:

*«Article 10 bis*

*Accès aux informations sur le compte de paiement par l'intermédiaire d'un prestataire de services d'information sur les comptes*

1. Les prestataires de services de paiement n'appliquent pas l'authentification forte du client lorsqu'un utilisateur de services de paiement accède en ligne à son compte de paiement par l'intermédiaire d'un prestataire de services d'information sur les comptes, à condition que cet accès soit limité à l'un des éléments suivants en ligne sans que des données de paiement sensibles soient divulguées:

   (a) le solde d'un ou de plusieurs comptes de paiement désignés;

   (b) les opérations de paiement exécutées durant les 90 derniers jours par l'intermédiaire d'un ou de plusieurs comptes de paiement désignés.

2. Par dérogation au paragraphe 1, les prestataires de services de paiement appliquent l'authentification forte du client lorsque l'une des conditions suivantes est remplie:

   (a) l'utilisateur de services de paiement accède en ligne aux informations visées au paragraphe 1 pour la première fois par l'intermédiaire du prestataire de services d'information sur les comptes;

(b) plus de 180 jours se sont écoulés depuis la dernière fois que l'utilisateur de services de paiement a accédé en ligne aux informations visées au paragraphe 1 par l'intermédiaire du prestataire de services d'information sur les comptes et que la procédure d'authentification forte du client a été appliquée.

3. Par dérogation au paragraphe 1, les prestataires de services de paiement sont autorisés à appliquer l'authentification forte du client lorsqu'un utilisateur de services de paiement accède en ligne à son compte de paiement par l'intermédiaire d'un prestataire de services d'information sur les comptes et que le prestataire de services de paiement a des raisons objectivement motivées et documentées liées à un accès non autorisé ou frauduleux au compte de paiement. Dans ce cas, le prestataire de services de paiement documente et motive dûment auprès de son autorité nationale compétente, sur demande, les raisons de l'application d'une authentification forte du client.

4. Les prestataires de services de paiement gestionnaires de comptes qui proposent une interface dédiée telle que visée à l'article 31 ne sont pas tenus d'appliquer la dérogation prévue au paragraphe 1 du présent article aux fins du mécanisme d'urgence visé à l'article 33, paragraphe 4, lorsqu'ils n'appliquent pas la dérogation prévue à l'article 10 dans l'interface directe utilisée pour l'authentification et la communication avec leurs utilisateurs de services de paiement.».

(3) À l'article 30, le paragraphe 4 *bis* suivant est inséré:

«4 *bis*. Par dérogation au paragraphe 4, les prestataires de services de paiement gestionnaires de comptes mettent à la disposition des prestataires de services de paiement visés dans le présent article les modifications apportées aux spécifications techniques de leurs interfaces pour se conformer à l'article 10 *bis*, au moins 2 mois avant la mise en œuvre de ces modifications.».

*Article 2*

***Dispositions transitoires***

1. Les prestataires de services de paiement qui appliquaient la dérogation prévue à l'article 10 du règlement délégué (UE) 2018/389 avant le... [JO: veuillez insérer la date correspondant à 7 mois après la date d'entrée en vigueur du présent règlement] sont autorisés à continuer d'appliquer cette dérogation pour les demandes d'accès reçues par l'intermédiaire d'un prestataire de services d'information sur les comptes jusqu'à l'expiration de la période couverte par cette dérogation.

2. Par dérogation au paragraphe 1, lorsqu'une nouvelle authentification forte du client est appliquée pour une demande d'accès par l'intermédiaire d'un prestataire de services d'information sur les comptes avant l'expiration de la période couverte par la dérogation visée au paragraphe 1, l'article 10 *bis* introduit par le présent règlement est applicable.

*Article 3*

***Entrée en vigueur et application***

Le présent règlement entre en vigueur le vingtième jour suivant celui de sa publication au *Journal officiel de l'Union européenne*.

Il est applicable à partir du ... [JO: veuillez insérer la date correspondant à 7 mois après la date d'entrée en vigueur du présent règlement].

Le présent règlement est obligatoire dans tous ses éléments et directement applicable dans tout État membre.

Fait à Bruxelles, le 3.8.2022

*Par la Commission*
*La présidente*
*Ursula VON DER LEYEN*