COMMISSION
EUROPÉENNE

Bruxelles, le 27.11.2017
C(2017) 7782 final

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

du XXX

complétant la directive 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

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

EXPOSÉ DES MOTIFS

1. CONTEXTE DE L'ACTE DÉLÉGUÉ

L'article 98, paragraphe 4, de la directive (UE) 2015/2366 habilite la Commission à adopter, à la suite de la soumission de projets de normes par l'Autorité bancaire européenne (ABE) et conformément aux articles 10 à 14 du règlement (UE) nº 1093/2010, des actes délégués précisant les exigences relatives à l'authentification forte du client, aux dérogations à l'application de celle-ci et à des normes ouvertes communes et sécurisées de communication.

Conformément à l'article 10, paragraphe 1, du règlement (UE) nº 1093/2010 instituant l'ABE, la Commission statue sur l'approbation d'un projet de norme dans les trois mois suivant sa réception. Elle peut aussi, lorsque l'intérêt de l'Union l'impose, n'approuver un projet de norme que partiellement ou moyennant des modifications, dans le respect de la procédure spécifique prévue audit article.

2. CONSULTATIONS AVANT L'ADOPTION DE L'ACTE

Conformément à l'article 10, paragraphe 1, troisième alinéa, du règlement (UE) nº 1093/2010, l'ABE a procédé à une consultation publique sur les projets de normes techniques soumis à la Commission en application de l'article 98, paragraphe 4, de la directive (UE) 2015/2366. Elle a publié un document de consultation sur son site internet le 12 août 2016; la consultation s'est achevée le 12 octobre 2016. Par ailleurs, l'ABE a demandé au groupe des parties intéressées au secteur bancaire, institué en application de l'article 37 du règlement (UE) nº 1093/2010, de rendre un avis sur ces projets de normes. Elle a présenté, en même temps que les projets de normes techniques, un document expliquant comment le résultat de ces consultations avait été pris en compte dans la version finale des projets de normes techniques soumise à la Commission.

Conformément à l'article 10, paragraphe 1, troisième alinéa, du règlement (UE) nº 1093/2010, l'ABE a joint aux projets de normes techniques soumis à la Commission son analyse d'impact, contenant notamment son analyse des coûts et des avantages qu'impliquent ces projets. Cette analyse est disponible à l'adresse https://www.eba.europa.eu/documents/10180/1761863/Final+draft+RTS+on+SCA+and+CSC+under+PSD2+%28EBA-RTS-2017-02%29.pdf, pp. 40-44 du paquet final de projets de normes techniques de réglementation.

3. ÉLÉMENTS JURIDIQUES DE L'ACTE DÉLÉGUÉ

Les présentes normes techniques de réglementation (NTR) précisent les exigences, en vertu de l'article 98 de la directive (UE) 2015/2366 (DSP2), relatives à l'authentification forte du client, les dérogations à l'application de celle-ci, les exigences auxquelles doivent satisfaire les mesures de sécurité afin de protéger la confidentialité et l'intégrité des données de sécurité personnalisées des utilisateurs de services de paiement, ainsi que les exigences applicables aux normes ouvertes communes et sécurisées de communication entre les prestataires de services de paiement gestionnaires de comptes, les prestataires de services d'initiation de paiement, les prestataires de services d'information sur les comptes, les payeurs, les bénéficiaires et d'autres prestataires de services de paiement.

Ces NTR tiennent compte des différents objectifs de la DSP2, à savoir notamment renforcer la sécurité, stimuler la concurrence, garantir la neutralité du modèle commercial et des technologies, contribuer à l'intégration des paiements dans l'UE, protéger les consommateurs, encourager l'innovation et améliorer la facilité d'utilisation pour le client.

Les NTR sont neutres sur le plan du modèle commercial et des technologies. Elles comportent un certain nombre de dérogations, notamment deux dérogations pour les paiements à distance: une concernant l'analyse des risques liés à l'opération et une autre concernant les paiements de faible valeur (moins de 30 EUR). Elles contiennent également des dérogations pour les paiements de proximité. Étant donné que la dérogation fondée sur l'analyse des risques liés à l'opération s'appuie sur le respect de taux de référence préétablis en matière de fraude, il convient que l'adéquation du ou des mécanisme(s) de contrôle du niveau de fraude du prestataire de services de paiement soit examinée par un contrôleur légal des comptes, afin de garantir l'évaluation impartiale de l'exactitude des données. Les niveaux de fraude effectivement atteints ne devraient pas uniquement être notifiés aux autorités compétentes, afin de garantir une mise en œuvre efficace des dérogations; ils devraient également être communiqués directement à l'ABE pour lui permettre d'effectuer un examen des taux de référence en matière de fraude figurant dans la NTR dans les 18 mois après l'entrée en vigueur de celle-ci.

Par rapport à la proposition de l'ABE, la Commission a prévu une dérogation supplémentaire à l'authentification forte du client, qui porte sur les opérations de paiement électronique réalisées par l'intermédiaire de procédures ou protocoles de paiement dédiés qui sont généralement utilisés par des entreprises et dont la sécurité est assurée par d'autres moyens que l'authentification d'une personne donnée. Cette dérogation est soumise à la condition que les autorités compétentes acquièrent la certitude que ces modes de paiement atteignent le niveau élevé de sécurité des paiements visé par la DSP2.

En raison même de leur nature, les paiements effectués par l'intermédiaire d'instruments de paiement anonymes ne sont pas soumis à l'obligation d'authentification forte du client. Il va sans dire que lorsque le caractère anonyme de ces instruments est supprimé pour des motifs contractuels ou législatifs, ces paiements sont soumis aux exigences de sécurité qui découlent de la DSP2 et de cette norme technique de réglementation.

Les NTR définissent également des exigences en matière de communication entre les prestataires de services de paiement gestionnaires de comptes, les prestataires de services d'information sur les comptes et les prestataires de services d'initiation de paiement, telles que l'obligation pour les premiers de proposer au moins une interface aux deuxièmes et troisièmes en vue de l'accès aux informations sur les comptes de paiement. Concernant la communication entre les prestataires de services de paiement gestionnaires de comptes, les prestataires de services d'information sur les comptes et les prestataires de services d'initiation de paiement, la pratique existante permettant l'accès de tiers sans identification, dénommée dans le jargon du marché «*screen scraping*» ou, erronément, «accès direct», ne sera par conséquent plus autorisée lorsque la période de transition prévue par l'article 115, paragraphe 4, de la DSP2 sera écoulée et que les NTR s'appliqueront. Cependant, les NTR fixent l'exigence pour les prestataires de services de paiement gestionnaires de comptes de développer et de maintenir une interface de communication permettant aux prestataires de services d'initiation de paiement, aux prestataires de services d'information sur les comptes et aux prestataires de services de paiement qui émettent des instruments de paiement liés à une carte d'accéder aux données dont ils ont besoin conformément à la DSP2. Les NTR s'appliquent uniquement aux comptes de paiement, conformément au champ d'application de la DSP2. Elles ne concernent donc pas l'accès à d'autres comptes que les comptes de paiement, qui relève de la compétence des États membres.

Lorsque le prestataire de services de paiement gestionnaire du compte décide d'utiliser une interface dédiée, la NTR impose qu'il définisse des indicateurs de performance clés et des valeurs cibles de niveau de service transparents pour cette interface. Ceux-ci doivent être au moins aussi exigeants que ceux fixés pour l'interface utilisée par les utilisateurs de services de paiement du prestataire de services de paiement gestionnaire du compte. Il doit par ailleurs publier les données sur une base trimestrielle.

Pour éviter que l’indisponibilité ou les performances insuffisantes de l’interface dédiée empêchent les prestataires de services d’initiation de paiement et les prestataires de services d’information sur les comptes de proposer leurs services aux utilisateurs, tandis que dans le même temps, les interfaces utilisateurs fonctionnent sans difficultés et permettent au prestataire de services de paiement gestionnaire du compte de proposer ses propres services de paiement, la Commission a modifié le projet de NTR de l’ABE afin de prévoir une mesure d’urgence sous la forme d’un mécanisme de secours. Celui-ci consiste à ouvrir les interfaces utilisateurs en tant que canal de communication sécurisé pour les prestataires de services d’initiation de paiement et les prestataires de services d’information sur les comptes. En cas de recours à cette mesure d’urgence, les dispositions pertinentes de la DSP2 (articles 65 à 67) s’appliquent aux prestataires de services d’initiation de paiement et aux prestataires de services d’information sur les comptes, y compris les procédures d’identification et d’authentification. Le recours à la mesure doit faire l’objet d’une description exhaustive par écrit et, à la demande, être notifiée aux autorités par les prestataires concernés.

Dans son avis sur les modifications apportées par la Commission, l’ABE a rejeté ce mécanisme de secours en avançant les deux arguments principaux suivants: le premier a trait au coût d’un tel mécanisme, qui devrait être supporté par les prestataires de services de paiement gestionnaires de comptes, en plus du coût d’interfaces dédiées performantes; le second est lié à la crainte de l’ABE qu’exiger un mécanisme de secours n’encouragerait pas la mise au point d’interfaces dédiées standardisées, étant donné que le mécanisme de secours suffirait à lui seul aux prestataires de services de paiement gestionnaires de comptes pour satisfaire aux exigences de la DSP2.

Compte tenu de l’avis de l’ABE, la Commission a révisé les modifications qu’elle avait apportées aux NTR, en maintenant le mécanisme de secours à titre de principe général, mais en habilitant les autorités nationales compétentes à exempter les banques de l’obligation de prévoir ce mécanisme si des conditions strictes sont remplies, garantissant que les interfaces dédiées ouvrent réellement le marché des services de paiement. Dès lors, les interfaces dédiées devront être testées par les prestataires de services de paiement qui les utiliseront et seront soumises à un test de résistance et contrôlées par les autorités compétentes. Si elles échouent lors des phases de test ou du test de résistance, les prestataires de services de paiement pourront recourir au mécanisme d’urgence prévu par les NTR.

Lorsqu’une interface dédiée a été exemptée de la mise en place du mécanisme d’urgence sur la base de l’interface client mais ne remplit plus les conditions d’une telle dérogation, ou qu’un prestataire de services de paiement gestionnaire de comptes ne propose pas d’interface répondant aux exigences de la DSP2 et des NTR, la Commission a prévu une disposition qui doit assurer la continuité des activités sur le marché des paiements. Dans ce cas, il incombera aux autorités compétentes de veiller à ce que les prestataires de services d’initiation de paiement et de services d’information sur les comptes ne soient pas bloqués ou entravés dans le cadre de la prestation de leurs services.

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

du XXX

complétant la directive 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

(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, et notamment son article 98, paragraphe 4, deuxième alinéa[1],

considérant ce qui suit:

(1) Les services de paiement proposés par voie électronique devraient être sécurisés, grâce à des technologies permettant de garantir une authentification sûre de l'utilisateur et de réduire, dans toute la mesure du possible, les risques de fraude. La procédure d'authentification devrait comprendre, en règle générale, des mécanismes de contrôle des opérations permettant de déceler les tentatives d'utiliser les données de sécurité personnalisées d'un utilisateur de services de paiement qui ont été perdues, volées ou détournées, et devrait également garantir que l'utilisateur de services de paiement est l'utilisateur légitime et donne dès lors son consentement au transfert de fonds et à l'accès aux informations sur son compte au travers d'une utilisation normale des données de sécurité personnalisées. Par ailleurs, il y a lieu de préciser les exigences relatives à l'authentification forte du client qui devraient être appliquées chaque fois qu'un payeur accède à son compte de paiement en ligne, initie une opération de paiement électronique ou exécute une action, grâce à un moyen de communication à distance, susceptible de comporter un risque de fraude en matière de paiement ou de toute autre utilisation frauduleuse, en imposant que soit généré un code d'authentification qui ne risque pas d'être falsifié, que ce soit dans son intégralité ou par la divulgation de l'un des éléments sur la base desquels il a été généré.

(2) Étant donné que les méthodes de fraude sont en constante évolution, les exigences relatives à l'authentification forte du client devraient permettre des solutions techniques innovantes répondant à l'émergence de nouvelles menaces pour la sécurité des paiements électroniques. Pour que les exigences à définir soient effectivement mises en œuvre sur une base continue, il convient également d'exiger que les mesures de sécurité pour l'application de l'authentification forte du client et ses dérogations, les mesures visant à protéger la confidentialité et l'intégrité des données de sécurité personnalisées et les mesures établissant des normes ouvertes communes et sécurisées de communication fassent l'objet d'une description exhaustive par écrit et soient

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

régulièrement testées, évaluées et contrôlées par des auditeurs possédant une expertise dans le domaine de la sécurité informatique et des paiements électroniques et indépendants sur le plan opérationnel. Pour permettre aux autorités compétentes de contrôler la qualité du réexamen de ces mesures, il convient que les résultats de ces réexamens soient mis à leur disposition à leur demande.

(3) Les opérations de paiement électronique à distance étant davantage exposées au risque de fraude, il est nécessaire de prévoir des exigences supplémentaires relatives à l'authentification forte des clients de ces opérations, qui garantissent que leurs éléments établissent un lien dynamique entre l'opération et un montant et un bénéficiaire précisés par le payeur lors de l'initiation de l'opération.

(4) L'établissement d'un lien dynamique est possible grâce à la génération de codes d'authentification, qui fait l'objet d'une série d'exigences strictes en matière de sécurité. Afin de maintenir la neutralité sur le plan des technologies, aucune technologie spécifique ne devrait être prescrite pour la mise en œuvre des codes d'authentification. Par conséquent, les codes d'authentification devraient être fondés sur des solutions telles que la génération et la validation de mots de passe à usage unique, de signatures numériques ou d'autres moyens de validation basés sur la cryptographie qui utilisent des clés ou du matériel cryptographique contenus dans les éléments d'authentification, pour autant que les exigences en matière de sécurité soient respectées.

(5) Il y a lieu de définir des exigences particulières pour les situations dans lesquelles le montant final n'est pas connu au moment où le payeur initie une opération de paiement électronique à distance, afin que l'authentification forte du client soit spécifique au montant maximal auquel le payeur a donné son consentement, conformément à la directive (UE) 2015/2366.

(6) Pour garantir l'application de l'authentification forte du client, il est également nécessaire d'exiger des caractéristiques de sécurité adéquates pour les éléments d'authentification forte du client appartenant à la catégorie «connaissance» (quelque chose que seul l'utilisateur connaît), comme la longueur ou la complexité, pour les éléments appartenant à la catégorie «possession» (quelque chose que seul l'utilisateur possède), comme les spécifications de l'algorithme, la longueur de la clé et l'entropie de l'information, et pour les dispositifs et logiciels qui lisent les éléments appartenant à la catégorie «inhérence» (quelque chose que l'utilisateur est), comme les spécifications de l'algorithme, le capteur biométrique et les dispositifs de protection des formats d'écran, notamment pour atténuer le risque que ces éléments soient mis au jour, divulgués à des tiers non autorisés et exploités par ceux-ci. Il convient également de définir les exigences visant à assurer l'indépendance de ces éléments, afin que la compromission de l'un ne remette pas en question la fiabilité des autres, notamment lorsque l'un de ces éléments est utilisé au travers d'un dispositif multifonctionnel, à savoir un dispositif tel une tablette ou un téléphone mobile, qui peut servir tant pour donner l'instruction d'effectuer le paiement que pour le processus d'authentification.

(7) Les exigences relatives à l'authentification forte du client s'appliquent aux paiements initiés par le payeur, que celui-ci soit une personne physique ou une entité juridique.

(8) En raison même de leur nature, les paiements effectués par l'intermédiaire d'instruments de paiement anonymes ne sont pas soumis à l'obligation d'authentification forte du client. Lorsque le caractère anonyme de ces instruments est supprimé pour des motifs contractuels ou législatifs, ces paiements sont soumis aux

exigences de sécurité qui découlent de la directive (UE) 2015/2366 et de cette norme technique de réglementation.

(9) Conformément à la directive (UE) 2015/2366, les dérogations au principe d'authentification forte du client ont été définies sur la base du niveau de risque, du montant, du caractère récurrent et du moyen utilisé pour exécuter l'opération de paiement.

(10) Les actions qui nécessitent l'accès au solde et aux opérations récentes d'un compte de paiement sans divulgation de données de paiement sensibles, les paiements récurrents aux mêmes bénéficiaires qui ont été préalablement créés ou confirmés par le payeur en recourant à l'authentification forte du client et les paiements en faveur ou en provenance de la même personne physique ou morale possédant des comptes auprès du même prestataire de services de paiement présentent un niveau de risque faible, qui permet aux prestataires de services de paiement de ne pas appliquer l'authentification forte du client. Il convient toutefois de rappeler qu'en vertu des articles 65, 66 et 67 de la directive (UE) 2015/2366, les prestataires de services d'initiation de paiement, les prestataires de services de paiement qui émettent des instruments de paiement liés à une carte et les prestataires de services d'information sur les comptes ne devraient demander au prestataire de services de paiement gestionnaire du compte les informations indispensables à la prestation d'un service de paiement donné, et ne les obtenir de lui, qu'avec le consentement de l'utilisateur des services de paiement. Ce consentement peut être donné individuellement pour chaque demande d'information ou chaque paiement à initier ou, pour les prestataires de services d'information sur les comptes, sous la forme d'un mandat pour les comptes de paiement désignés et les opérations de paiement associées définis dans l'accord contractuel avec l'utilisateur de services de paiement.

(11) Des dérogations pour les paiements sans contact de faible valeur au point de vente, qui autorisent aussi un nombre maximal ou une valeur fixe maximale d'opérations consécutives sans authentification forte du client, permettent le développement de services de paiement conviviaux présentant un faible risque et devraient dès lors être prévues. Il y a également lieu de prévoir une dérogation pour les opérations de paiement électronique initiées à partir d'automates de paiement, pour lesquelles le recours à l'authentification forte du client est susceptible de ne pas être toujours aisé à appliquer pour des motifs opérationnels (par exemple, pour éviter les files d'attente et les éventuels accidents aux gares de péage ou en raison d'autres risques pour la sûreté ou la sécurité).

(12) Comme dans le cas de la dérogation applicable aux paiements sans contact de faible valeur au point de vente, il convient de trouver un juste équilibre entre l'intérêt d'un renforcement de la sécurité des paiements à distance et les besoins de convivialité et d'accessibilité des paiements dans le secteur du commerce électronique. Conformément à ces principes, les seuils au-dessous desquels il n'est pas nécessaire d'appliquer l'authentification forte du client devraient être fixés avec prudence, afin de se limiter aux seuls achats en ligne de faible valeur. Les seuils applicables aux achats en ligne devraient être fixés plus prudemment, étant donné que le fait que la personne n'est pas présente physiquement lors de la réalisation de l'achat présente un risque légèrement plus élevé en matière de sécurité.

(13) Les exigences relatives à l'authentification forte du client s'appliquent aux paiements initiés par le payeur, que celui-ci soit une personne physique ou une entité juridique. De nombreux paiements effectués par les entreprises sont initiés au moyen de

procédures ou protocoles dédiés qui garantissent les niveaux élevés de sécurité des paiements que la directive (UE) 2015/2366 vise à atteindre grâce à l'authentification forte du client. Lorsque les autorités compétentes établissent que ces procédures et protocoles de paiement, qui sont uniquement mis à la disposition de payeurs qui ne sont pas des consommateurs, satisfont aux objectifs de la directive (UE) 2015/2366 sur le plan de la sécurité, les prestataires de services de paiement peuvent, en ce qui concerne ces procédures ou protocoles, être exemptés des exigences relatives à l'authentification forte du client.

(14) Si une analyse en temps réel des risques liés à l'opération classe une opération de paiement comme présentant peu de risques, il convient également d'instaurer une dérogation pour le prestataire de services de paiement qui entend ne pas appliquer l'authentification forte du client, en adoptant des exigences efficaces et fondées sur les risques qui garantissent la sécurité des fonds et des données à caractère personnel de l'utilisateur de services de paiement. Ces exigences fondées sur les risques devraient combiner les résultats de l'analyse des risques («*risk scoring*»), confirmant qu'aucune dépense ou aucun type de comportement anormal du payeur n'a été décelé, en tenant compte d'autres facteurs de risque tels que les informations sur la localisation du payeur et du bénéficiaire, avec les seuils en valeur liés aux taux de fraude calculés pour les paiements à distance. Lorsque, sur la base de l'analyse en temps réel des risques liés à l'opération, un paiement ne peut être considéré comme présentant peu de risques, le prestataire de services de paiement devrait revenir à l'authentification forte du client. Le montant maximal de cette dérogation fondée sur les risques devrait être fixé de telle manière qu'il corresponde à un taux de fraude très faible, même en comparaison des taux de fraude de l'ensemble des opérations de paiement du prestataire de services de paiement, y compris ceux authentifiés grâce à l'authentification forte du client, au cours d'une certaine période et sur une base glissante.

(15) Afin d'assurer une application effective, les prestataires de services de paiement qui souhaitent bénéficier des dérogations à l'authentification forte du client devraient régulièrement contrôler et mettre à la disposition des autorités compétentes et de l'Autorité bancaire européenne (ABE), à leur demande, et pour chaque type d'opération de paiement, la valeur des opérations frauduleuses ou non autorisées et les taux de fraude observés pour l'ensemble de leurs opérations de paiement, que celles-ci aient été authentifiées grâce à l'authentification forte du client ou exécutées dans le cadre d'une dérogation.

(16) La collecte de ces nouvelles données historiques sur les taux de fraude des opérations de paiement électronique contribuera également à un réexamen effectif par l'ABE des seuils applicables aux dérogations à l'authentification forte du client sur la base d'une analyse en temps réel des risques liés à l'opération. Conformément à l'article 98, paragraphe 5, de la directive (UE) 2015/2366 et à l'article 10 du règlement (UE) nº 1093/2010 du Parlement européen et du Conseil[2], l'ABE devrait réexaminer les présentes normes techniques de réglementation et, le cas échéant, soumettre des projets de mise à jour à la Commission, en présentant de nouveaux projets de seuils et

[2] 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).

de taux de fraude correspondants, dans le but d'améliorer la sécurité des paiements électroniques à distance.

(17) Les prestataires de services de paiement qui feront usage des dérogations à prévoir devraient être autorisés, à tout moment, à choisir l'authentification forte du client pour les actions et les opérations de paiement visées dans ces dispositions.

(18) Les mesures qui protègent la confidentialité et l'intégrité des données de sécurité personnalisées, ainsi que les dispositifs et logiciels d'authentification, devraient limiter les risques liés à la fraude commise au moyen de l'utilisation non autorisée ou frauduleuse d'instruments de paiement et l'accès non autorisé à des comptes de paiement. À cette fin, il est nécessaire d'introduire des exigences concernant la création et la livraison sécurisées des données de sécurité personnalisées et leur association à l'utilisateur de services de paiement, et de prévoir des conditions pour le renouvellement et la désactivation de ces données.

(19) Afin d'assurer une communication efficace et sécurisée entre les acteurs concernés dans le contexte des services d'information sur les comptes, des services d'initiation des paiements et de la confirmation de la disponibilité des fonds, il y a lieu de préciser les exigences relatives aux normes ouvertes communes et sécurisées de communication auxquelles doivent satisfaire tous les prestataires de services de paiement concernés. La directive (UE) 2015/2366 prévoit l'accès aux informations sur les comptes de paiement et leur utilisation par les prestataires de services d'information sur les comptes. Le présent règlement ne modifie par conséquent pas les règles d'accès aux comptes qui ne sont pas des comptes de paiement.

(20) Chaque prestataire de services de paiement gestionnaire de comptes qui gère des comptes de paiement accessibles en ligne devrait proposer au moins une interface d'accès permettant une communication sécurisée avec les prestataires de services d'information sur les comptes, les prestataires de services d'initiation de paiement et les prestataires de services de paiement qui émettent des instruments de paiement liés à une carte. Cette interface devrait permettre aux prestataires de services d'information sur les comptes, aux prestataires de services d'initiation de paiement et aux prestataires de services de paiement qui émettent des instruments de paiement liés à une carte de s'identifier auprès du prestataire de services de paiement gestionnaire du compte. Elle devrait également permettre aux prestataires de services d'information sur les comptes et aux prestataires de services d'initiation de paiement de s'appuyer sur les procédures d'authentification proposées par le prestataire de services de paiement gestionnaire du compte à l'utilisateur de services de paiement. Pour garantir la neutralité du modèle commercial et des technologies, les prestataires de services de paiement gestionnaires de comptes devraient être libres de décider s'ils proposent une interface dédiée à la communication avec les prestataires de services d'information sur les comptes, les prestataires de services d'initiation de paiement et les prestataires de services de paiement qui émettent des instruments de paiement liés à une carte ou s'ils autorisent, pour cette communication, le recours à l'interface servant à l'identification des utilisateurs de services de paiement des prestataires de services de paiement gestionnaires de comptes et à la communication avec ces utilisateurs.

(21) Pour permettre aux prestataires de services d'information sur les comptes, aux prestataires de services d'initiation de paiement et aux prestataires de services de paiement qui émettent des instruments de paiement liés à une carte de mettre au point leurs solutions techniques, les spécifications techniques de l'interface devraient être dûment consignées par écrit et publiées. Par ailleurs, le prestataire de services de

paiement gestionnaire du compte devrait proposer un dispositif permettant aux prestataires de services de paiement de tester les solutions techniques au moins six mois avant la date d'application des présentes normes de réglementation ou, si le lancement a lieu après la date d'application des présentes normes, avant la date à laquelle l'interface sera lancée sur le marché. Afin de garantir l'interopérabilité des différentes solutions de communication technologiques, l'interface devrait utiliser des normes de communication mises au point par des organisations européennes ou internationales de normalisation.

(22) La qualité des services fournis par les prestataires de services d'information sur les comptes et les prestataires de services d'initiation de paiement dépendra du bon fonctionnement des interfaces mises en place ou adaptées par les prestataires de services de paiement gestionnaires de comptes. Il importe par conséquent, si ces interfaces ne sont pas conformes aux dispositions figurant dans les présentes normes, que des mesures soient prises pour assurer la continuité des activités au profit des utilisateurs de ces services. Il incombe aux autorités nationales compétentes de veiller à ce que les prestataires de services d'information sur les comptes et les prestataires de services d'initiation de paiement ne soient pas bloqués ou entravés dans le cadre de la prestation de leurs services.

(23) Lorsque l'accès aux comptes de paiement est proposé au moyen d'une interface dédiée, il convient, pour garantir le droit des utilisateurs de services de paiement de recourir à des prestataires de services d'initiation de paiement et à des services permettant l'accès aux données des comptes, conformément à la directive (UE) 2015/2366, d'exiger que l'interface dédiée ait le même niveau de disponibilité et de performances que l'interface à la disposition de l'utilisateur de services de paiement. Les prestataires de services de paiement gestionnaires de comptes devraient également définir des indicateurs de performance clés et des valeurs cibles de niveau de service transparents concernant la disponibilité et les performances des interfaces dédiées qui soient au moins aussi exigeants que ceux fixés pour l'interface utilisée par leurs utilisateurs de services de paiement. Ces interfaces devaient être testées par les prestataires de services de paiement qui les utiliseront et devraient être soumises à un test de résistance et contrôlées par les autorités compétentes.

(24) Pour que les prestataires de services de paiement qui ont recours à l'interface dédiée puissent continuer à fournir leurs services en cas de problèmes de disponibilité ou de performances insuffisantes, il y a lieu de prévoir, sous réserve de conditions strictes, un mécanisme de secours qui permettra à ces prestataires d'utiliser l'interface dont le prestataire de services de paiement gestionnaire du compte dispose pour l'identification de ses propres utilisateurs de services de paiement et la communication avec ceux-ci. Certains prestataires de services de paiement gestionnaires de comptes seront exemptés de l'obligation de proposer un tel mécanisme de secours par l'intermédiaire de leurs interfaces clients, si leurs autorités compétentes établissent que leurs interfaces dédiées satisfont à des conditions spécifiques assurant une concurrence sans entraves. Dans le cas où les interfaces dédiées exemptées ne satisferaient pas aux conditions requises, les dérogations octroyées doivent être annulées par les autorités compétentes concernées.

(25) Afin que les autorités compétentes puissent surveiller et contrôler efficacement la mise en œuvre et la gestion des interfaces de communication, il convient que les prestataires de services de paiement gestionnaires de comptes mettent une synthèse de la documentation correspondante à disposition sur leur site internet et fournissent, à la demande, aux autorités compétentes une documentation sur les solutions en cas

d'urgence. Les prestataires de services de paiement gestionnaires de comptes devraient également publier les statistiques relatives à la disponibilité et aux performances de ces interfaces.

(26) Pour préserver la confidentialité et l'intégrité des données, il est nécessaire d'assurer la sécurité des sessions de communication entre les prestataires de services de paiement gestionnaires de comptes, les prestataires de services d'information sur les comptes, les prestataires de services d'initiation de paiement et les prestataires de services de paiement qui émettent des instruments de paiement liés à une carte. Il convient tout particulièrement d'exiger qu'un cryptage sécurisé soit utilisé entre les prestataires de services d'information sur les comptes, les prestataires de services d'initiation de paiement, les prestataires de services de paiement qui émettent des instruments de paiement liés à une carte et les prestataires de services de paiement gestionnaires de comptes lorsqu'ils échangent des données.

(27) Pour renforcer la confiance des utilisateurs et assurer l'authentification forte du client, l'utilisation de moyens d'identification électronique et de services de confiance tels que définis dans le règlement (UE) nº 910/2014 du Parlement européen et du Conseil[3] devrait être prise en compte, notamment en ce qui concerne les schémas d'identification électronique notifiés.

(28) Pour que les dates d'application soient alignées, il convient que le présent règlement soit applicable à partir de la date à laquelle les États membres doivent assurer l'application des mesures de sécurité visées aux articles 65, 66, 67 et 97 de la directive 2015/2366.

(29) Le présent règlement se fonde sur les projets de normes techniques de réglementation soumis à la Commission par l'Autorité bancaire européenne (ci-après l'«ABE»).

(30) L'ABE a procédé à des consultations publiques ouvertes et transparentes 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 en application de l'article 37 du règlement (UE) nº 1093/2010,

A ADOPTÉ LE PRÉSENT RÈGLEMENT:

CHAPITRE I
DISPOSITIONS GÉNÉRALES

Article premier
Objet

Le présent règlement fixe les exigences auxquelles les prestataires de services de paiement doivent satisfaire pour mettre en œuvre les mesures de sécurité leur permettant d'effectuer les actions suivantes:

(a) appliquer la procédure d'authentification forte du client conformément à l'article 97 de la directive (UE) 2015/2366;

[3] Règlement (UE) nº 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE (JO L 257 du 28.8.2014, p. 53).

(b) déroger à l'application des exigences de sécurité relatives à l'authentification forte du client, sous réserve de conditions bien définies et limitées fondées sur le niveau de risque, le montant et le caractère récurrent de l'opération de paiement et le moyen utilisé pour l'exécuter;

(c) protéger la confidentialité et l'intégrité des données de sécurité personnalisées de l'utilisateur de services de paiement;

(d) établir des normes ouvertes communes et sécurisées de communication entre les prestataires de services de paiement gestionnaires de comptes, les prestataires de services d'initiation de paiement, les prestataires de services d'information sur les comptes, les payeurs, les bénéficiaires et d'autres prestataires de services de paiement en ce qui concerne la prestation et l'utilisation de services de paiement en application du titre IV de la directive (UE) 2015/2366.

Article 2
Exigences générales en matière d'authentification

1. Les prestataires de services de paiement mettent en place des mécanismes de contrôle des opérations qui leur permettent de déceler les opérations de paiement non autorisées ou frauduleuses aux fins de la mise en œuvre des mesures de sécurité visées aux points a) et b) de l'article 1er.

Ces mécanismes sont fondés sur l'analyse d'opérations de paiement tenant compte d'éléments qui sont propres à l'utilisateur de services de paiement dans des conditions d'utilisation normale des données de sécurité personnalisées.

2. Les prestataires de services de paiement veillent à ce que les mécanismes de contrôle des opérations tiennent au moins compte de chacun des facteurs suivants liés aux risques:

(a) les listes d'éléments d'authentification volés ou détournés;

(b) le montant de chaque opération de paiement;

(c) les scénarios connus de fraude lors de la prestation de services de paiement;

(d) les signes d'infection par un logiciel malveillant lors de sessions d'application de la procédure d'authentification;

(e) si le dispositif d'accès ou le logiciel est fourni par le prestataire de services de paiement, un registre d'utilisation du dispositif d'accès ou du logiciel fourni à l'utilisateur de services de paiement et de l'utilisation anormale du dispositif ou du logiciel.

Article 3
Examen des mesures de sécurité

1. La mise en œuvre des mesures de sécurité visées à l'article 1er est décrite par écrit, testée régulièrement, évaluée et contrôlée, conformément au cadre juridique applicable au prestataire de services de paiement, par des auditeurs possédant une expertise dans le domaine de la sécurité informatique et des paiements électroniques et indépendants sur le plan opérationnel au sein du prestataire de services de paiement ou vis-à-vis de celui-ci.

2. Le délai entre les audits visés au paragraphe 1 est déterminé compte tenu du cadre comptable et du contrôle légal des comptes correspondant qui est applicable au prestataire de services de paiement.

Toutefois, les prestataires de services de paiement qui font usage de la dérogation visée à l'article 18 font l'objet au moins une fois par an d'un audit portant sur la méthodologie, le modèle et les taux de fraude notifiés. L'auditeur qui réalise cet audit possède une expertise dans le domaine de la sécurité informatique et des paiements électroniques et est indépendant sur le plan opérationnel au sein du prestataire de services de paiement ou vis-à-vis de celui-ci. Au cours de la première année où il est fait usage de la dérogation visée à l'article 18, et au moins tous les trois ans ensuite, ou plus fréquemment si l'autorité compétente le demande, cet audit est réalisé par un auditeur externe indépendant et qualifié.

3. Cet audit évalue et rend compte de la conformité des mesures de sécurité du prestataire de services de paiement avec les exigences fixées par le présent règlement.

L'intégralité du rapport est mise à la disposition des autorités compétentes à la demande de celles-ci.

CHAPITRE II
MESURES DE SÉCURITÉ POUR L'APPLICATION DE LA PROCÉDURE D'AUTHENTIFICATION FORTE DU CLIENT

Article 4
Code d'authentification

1. Lorsque les prestataires de services de paiement appliquent la procédure d'authentification forte du client conformément à l'article 97, paragraphe 1, de la directive (UE) 2015/2366, l'authentification est fondée sur deux ou plusieurs éléments appartenant aux catégories «connaissance», «possession» et «inhérence» et donne lieu à la génération d'un code d'authentification.

   Le code d'authentification n'est accepté qu'une seule fois par le prestataire de services de paiement lorsque le payeur utilise ce code pour accéder à son compte de paiement en ligne, pour initier une opération de paiement électronique ou pour exécuter une action, grâce à un moyen de communication à distance, susceptible de comporter un risque de fraude en matière de paiement ou de toute autre utilisation abusive.

2. Aux fins du paragraphe 1, les prestataires de services de paiement prennent des mesures de sécurité garantissant le respect de chacune des exigences suivantes:

   (a) aucune information sur l'un des éléments visés au paragraphe 1 ne peut être déduite de la divulgation du code d'authentification;

   (b) il n'est pas possible de générer un nouveau code d'authentification en se basant sur un autre code d'authentification généré au préalable;

   (c) le code d'authentification ne peut pas être falsifié.

3. Les prestataires de services de paiement veillent à ce que l'authentification au moyen de la génération d'un code d'authentification intègre chacune des mesures suivantes:

   (a) lorsque l'authentification pour accès à distance, paiements électroniques à distance et toute autre action grâce à un moyen de communication à distance susceptible de comporter un risque de fraude en matière de paiement ou de toute autre utilisation abusive n'a pas généré de code d'authentification aux fins du paragraphe 1, il n'est pas possible de déterminer lequel des éléments visés dans ledit paragraphe était incorrect;

   (b) le nombre de tentatives d'authentification infructueuses consécutives au bout duquel les actions prévues à l'article 97, paragraphe 1, de la directive (UE) 2015/2366 sont bloquées à titre temporaire ou permanent ne dépasse pas cinq au cours d'une période donnée;

   (c) les sessions de communication sont protégées contre l'interception des données d'authentification communiquées durant l'authentification et contre la manipulation par des tiers non autorisés, conformément aux exigences du chapitre V;

   (d) le délai maximal d'inactivité du payeur, une fois que celui-ci s'est authentifié pour accéder à son compte de paiement en ligne, ne dépasse pas cinq minutes.

4. Si le blocage visé au paragraphe 3, point b), est temporaire, la durée de celui-ci et le nombre de nouveaux essais sont fixés sur la base des caractéristiques du service

fourni au payeur et de l'ensemble des risques correspondants qui y sont associés, en tenant compte, au minimum, des facteurs énoncés à l'article 2, paragraphe 2.

Le payeur est averti avant que le blocage ne devienne permanent.

Lorsque le blocage est rendu permanent, une procédure sécurisée est mise en place pour permettre au payeur d'utiliser à nouveau les instruments de paiement électronique bloqués.

Article 5
Établissement d'un lien dynamique

1. Lorsqu'ils appliquent la procédure d'authentification forte du client conformément à l'article 97, paragraphe 2, de la directive (UE) 2015/2366, les prestataires de services de paiement, outre les éléments exigés à l'article 4 du présent règlement, prennent également des mesures de sécurité qui satisfont à chacune des exigences suivantes:

   (a) le payeur est informé du montant de l'opération de paiement et du bénéficiaire;

   (b) le code d'authentification généré est spécifique au montant de l'opération de paiement et au bénéficiaire approuvé par le payeur lors de l'initiation de l'opération;

   (c) le code d'authentification accepté par le prestataire de services de paiement correspond au montant spécifique initial de l'opération de paiement et à l'identité du bénéficiaire approuvé par le payeur;

   (d) toute modification du montant ou du bénéficiaire entraîne l'invalidation du code d'authentification généré.

2. Aux fins du paragraphe 1, les prestataires de services de paiement prennent des mesures de sécurité garantissant la confidentialité, l'authenticité et l'intégrité de chacun des éléments suivants:

   (a) le montant de l'opération et le bénéficiaire durant l'ensemble des phases de l'authentification;

   (b) les informations qui s'affichent pour le payeur durant l'ensemble des phases de l'authentification, y compris la génération, la transmission et l'utilisation du code d'authentification.

3. Aux fins du paragraphe 1, point b), et lorsque les prestataires de services de paiement appliquent l'authentification forte du client conformément à l'article 97, paragraphe 2, de la directive (UE) 2015/2366, les exigences suivantes sont applicables au code d'authentification:

   (a) en ce qui concerne les opérations de paiement liées à une carte pour lesquelles le payeur a donné son consentement quant au montant exact des fonds à bloquer en vertu de l'article 75, paragraphe 1, de ladite directive, le code d'authentification est spécifique au montant au blocage duquel le payeur a donné son consentement et que le payeur a approuvé lors de l'initiation de l'opération;

   (b) en ce qui concerne les opérations de paiement pour lesquelles le payeur a donné son consentement à l'exécution d'une série d'opérations de paiement électronique à distance en faveur d'un ou de plusieurs bénéficiaires, le code d'authentification est spécifique au montant total de la série d'opérations de paiement et aux bénéficiaires désignés.

Article 6

Exigences relatives aux éléments appartenant à la catégorie «connaissance»

1. Les prestataires de services de paiement prennent des mesures pour atténuer le risque que les éléments d'authentification forte du client appartenant à la catégorie «connaissance» ne soient mis au jour par des tiers non autorisés ou divulgués à ceux-ci.

2. L'utilisation par le payeur de ces éléments fait l'objet de mesures d'atténuation des risques visant à éviter leur divulgation à des tiers non autorisés.

Article 7

Exigences relatives aux éléments appartenant à la catégorie «possession»

1. Les prestataires de services de paiement prennent des mesures pour atténuer le risque que les éléments d'authentification forte du client appartenant à la catégorie «possession» ne soient utilisés par des tiers non autorisés.

2. L'utilisation par le payeur de ces éléments fait l'objet de mesures visant à éviter leur copie.

Article 8

Exigences relatives aux dispositifs et logiciels associés à des éléments appartenant à la catégorie «inhérence»

1. Les prestataires de services de paiement prennent des mesures pour atténuer le risque que des éléments d'authentification appartenant à la catégorie «inhérence» qui sont lus par des dispositifs et logiciels d'accès fournis au payeur ne soient mis au jour par des tiers non autorisés. Au minimum, les prestataires de services de paiement veillent à ce qu'il soit très peu probable, avec ces dispositifs et logiciels d'accès, qu'un tiers non autorisé soit authentifié comme étant le payeur.

2. L'utilisation par le payeur de ces éléments fait l'objet de mesures garantissant que ces dispositifs et logiciels empêchent toute utilisation non autorisée desdits éléments qui passerait par un accès à ces dispositifs et logiciels.

Article 9

Indépendance des éléments

1. Les prestataires de services de paiement veillent à ce que l'utilisation des éléments d'authentification forte du client visés aux articles 6, 7 et 8 fasse l'objet de mesures garantissant que sur le plan de la technologie, des algorithmes et des paramètres, la compromission d'un des éléments ne remet pas en question la fiabilité des autres.

2. Les prestataires de services de paiement prennent des mesures de sécurité, lorsque l'un des éléments d'authentification forte du client ou le code d'authentification proprement dit est utilisé au travers d'un dispositif multifonctionnel, pour réduire le risque qui découlerait de l'altération de ce dispositif multifonctionnel.

3. Aux fins du paragraphe 2, les mesures d'atténuation prévoient chacun des éléments suivants:

   (a) l'utilisation d'environnements d'exécution sécurisés distincts grâce au logiciel installé sur le dispositif multifonctionnel;

(b) des mécanismes permettant de garantir que le logiciel ou le dispositif n'a pas été altéré par le payeur ou par un tiers;

(c) en cas d'altérations, des mécanismes permettant de réduire les conséquences de celles-ci.

CHAPITRE III
DÉROGATIONS À L'OBLIGATION D'AUTHENTIFICATION FORTE DU CLIENT

Article 10
Information sur le compte de paiement

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 et au paragraphe 2 du présent article, lorsqu'un utilisateur de services de paiement est limité dans son accès à un ou deux 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. Aux fins du 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 du service de paiement accède pour la première fois en ligne aux informations visées au paragraphe 1;

(b) plus de 90 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, point b), et que la procédure d'authentification forte du client a été appliquée.

Article 11
Paiement sans contact au point de vente

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, lorsque le payeur initie une opération de paiement électronique sans contact, pour autant que les conditions suivantes soient remplies:

(a) le montant individuel de l'opération de paiement électronique sans contact ne dépasse pas 50 EUR; et

(b) le montant cumulé des précédentes opérations de paiement électronique sans contact initiées par l'intermédiaire d'un instrument de paiement disposant d'une fonctionnalité sans contact, depuis la date de la dernière authentification forte du client, ne dépasse pas 150 EUR; ou

(c) le nombre d'opérations de paiement électronique sans contact consécutives initiées par l'intermédiaire de l'instrument de paiement disposant d'une fonctionnalité sans contact, depuis la dernière authentification forte du client, ne dépasse pas cinq.

Article 12
Automates de paiement des frais de transport et de parking

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, lorsque le payeur initie une opération de paiement électronique à partir d'un automate de paiement, afin de régler des frais de transport ou de parking.

Article 13
Bénéficiaires de confiance

1. Les prestataires de services de paiement appliquent l'authentification forte du client lorsqu'un payeur crée ou modifie une liste de bénéficiaires de confiance par l'intermédiaire du prestataire de services de paiement gestionnaire de son compte.
2. Les prestataires de services de paiement sont autorisés à ne pas appliquer l'authentification forte du client, sous réserve du respect des exigences générales en matière d'authentification, lorsque le payeur initie une opération de paiement et que le bénéficiaire figure dans une liste de bénéficiaires de confiance préalablement créée par le payeur.

Article 14
Opérations récurrentes

1. Les prestataires de services de paiement appliquent l'authentification forte du client lorsqu'un payeur crée, modifie ou initie pour la première fois une série d'opérations récurrentes ayant le même montant et le même bénéficiaire.
2. Les prestataires de services de paiement sont autorisés à ne pas appliquer l'authentification forte du client, sous réserve du respect des exigences générales en matière d'authentification, pour l'initiation de l'ensemble des opérations de paiement ultérieures comprises dans la série d'opérations de paiement visées au paragraphe 1.

Article 15
Virements entre comptes détenus par la même personne physique ou morale

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, lorsque le payeur initie un virement pour lequel le payeur et le bénéficiaire sont la même personne physique ou morale et les deux comptes de paiement sont détenus auprès du même prestataire de services de paiement gestionnaire du compte.

Article 16
Opérations de faible valeur

Les prestataires de services de paiement sont autorisés à ne pas appliquer l'authentification forte du client lorsque le payeur initie une opération de paiement électronique à distance, pour autant que les conditions suivantes soient remplies:

(a) le montant de l'opération de paiement électronique à distance ne dépasse pas 30 EUR; et

(b) le montant cumulé des précédentes opérations de paiement électronique à distance initiées par le payeur depuis la dernière authentification forte du client ne dépasse pas 100 EUR; ou

(c) le nombre des précédentes opérations de paiement électronique à distance initiées par le payeur depuis la dernière authentification forte du client ne dépasse pas 5 opérations de paiement électronique à distance individuelles consécutives.

Article 17

Procédures et protocoles de paiement sécurisés utilisés par les entreprises

Les prestataires de services de paiement sont autorisés à ne pas appliquer l'authentification forte du client à l'égard de personnes morales qui initient des opérations de paiement électronique au moyen de procédures ou de protocoles de paiement dédiés qui sont uniquement mis à la disposition de payeurs qui ne sont pas des consommateurs, lorsque les autorités compétentes ont acquis la certitude que lesdits procédures et protocoles garantissent des niveaux de sécurité au moins équivalents à ceux prévus par la directive 2015/2366.

Article 18

Analyse des risques liés à l'opération

1. Les prestataires de services de paiement sont autorisés à ne pas appliquer l'authentification forte du client lorsque le payeur initie une opération de paiement électronique à distance que le prestataire de services de paiement considère comme présentant un faible niveau de risque conformément aux mécanismes de contrôle des opérations visés à l'article 2 et au paragraphe 2, point c), du présent article.

2. Une opération de paiement électronique visée au paragraphe 1 est considérée comme présentant un faible niveau de risque lorsque l'ensemble des conditions suivantes sont remplies:

   (a) le taux de fraude pour ce type d'opération, tel que notifié par le prestataire de services de paiement et calculé conformément à l'article 19, est équivalent ou inférieur aux taux de référence en matière de fraude mentionnés dans le tableau figurant à l'annexe pour les «paiements électroniques à distance liés à une carte» et les «virements électroniques à distance» respectivement;

   (b) le montant de l'opération ne dépasse pas la valeur-seuil de dérogation correspondante mentionnée dans le tableau figurant à l'annexe;

   (c) les prestataires de services de paiement n'ont décelé aucun des éléments suivants à l'issue d'une analyse en temps réel des risques:

      i) des dépenses anormales ou un type de comportement anormal du payeur;

      ii) des informations inhabituelles concernant l'utilisation du dispositif ou logiciel du payeur à des fins d'accès;

      iii) des signes d'infection par un logiciel malveillant lors d'une session de la procédure d'authentification;

      iv) un scénario connu de fraude dans le cadre de la prestation de services de paiement;

      v) une localisation anormale du payeur;

      vi) une localisation du bénéficiaire présentant des risques élevés.

3. Les prestataires de services de paiement qui entendent exempter des opérations de paiement électronique à distance de l'authentification forte du client au motif qu'elles présentent un risque faible tiennent au moins compte des facteurs suivants liés aux risques:

(a) les habitudes de dépenses antérieures de l'utilisateur individuel de services de paiement;

(b) l'historique des opérations de paiement de chacun des utilisateurs de services de paiement du prestataire de services de paiement;

(c) la localisation du payeur et du bénéficiaire au moment de l'opération de paiement dans les cas où le dispositif d'accès ou le logiciel est fourni par le prestataire de services de paiement;

(d) l'identification de comportements de paiement anormaux de l'utilisateur de services de paiement par rapport à l'historique de ses opérations de paiement.

L'évaluation du prestataire de services de paiement intègre l'ensemble de ces facteurs liés aux risques dans une note de risque, attribuée à chaque opération individuelle, qui permet de déterminer s'il convient d'autoriser un paiement spécifique sans authentification forte du client.

Article 19
Calcul des taux de fraude

1. Pour chaque type d'opération visé dans le tableau figurant en annexe, le prestataire de services de paiement veille à ce que les taux de fraude globaux liés tant aux opérations de paiement authentifiées par une authentification forte du client qu'à celles effectuées au titre des dérogations visées aux articles 13 à 18 soient équivalents ou inférieurs au taux de référence en matière de fraude lié au même type d'opération de paiement qui est mentionné dans le tableau figurant en annexe.

Le taux de fraude global lié à chaque type d'opération est calculé comme étant la valeur totale des opérations à distance non autorisées ou frauduleuses, dont les fonds ont été récupérés ou pas, divisée par la valeur totale de l'ensemble des opérations à distance pour le même type d'opérations, authentifiées par une authentification forte du client ou exécutées au titre d'une dérogation visée aux articles 13 à 18, sur une base trimestrielle glissante (90 jours).

2. Le calcul des taux de fraude et les chiffres qui en découlent sont évalués dans le cadre de l'audit visé à l'article 3, paragraphe 2, qui en assure l'exhaustivité et l'exactitude.

3. La méthode et tout modèle qu'utilise le prestataire de services de paiement pour calculer les taux de fraude, ainsi que les taux de fraude proprement dits, sont dûment consignés par écrit et mis à l'entière disposition des autorités compétentes et de l'ABE, moyennant notification préalable à l'(aux) autorité(s) compétente(s), à leur demande.

Article 20
Suspension des dérogations sur la base de l'analyse des risques liés à l'opération

1. Les prestataires de services de paiement qui font usage de la dérogation visée à l'article 18 préviennent immédiatement les autorités compétentes si l'un des taux de fraude qu'ils contrôlent, pour tout type d'opérations de paiement indiqué dans le

tableau figurant en annexe, dépasse le taux de référence applicable en matière de fraude, et fournissent aux autorités compétentes une description des mesures qu'ils entendent prendre pour rétablir la conformité du taux de fraude en question avec les taux de référence applicables en matière de fraude.

2. Les prestataires de services de paiement cessent immédiatement de faire usage de la dérogation visée à l'article 18 pour tout type d'opération de paiement indiqué dans le tableau figurant en annexe dans la fourchette de seuils de dérogation concernée, lorsque le taux de fraude qu'ils contrôlent dépasse pendant deux trimestres consécutifs le taux de référence en matière de fraude applicable à cet instrument de paiement ou à ce type d'opération de paiement à l'intérieur de cette fourchette.

3. Après la suspension, conformément au paragraphe 2 du présent article, de la dérogation visée à l'article 18, les prestataires de services de paiement ne font à nouveau usage de cette dérogation que lorsque leur taux de fraude calculé reste égal ou inférieur, pendant un trimestre, aux taux de référence en matière de fraude applicables à ce type d'opération de paiement dans la fourchette de seuils de dérogation.

4. S'ils entendent faire à nouveau usage de la dérogation visée à l'article 18, les prestataires de services de paiement en informent les autorités compétentes dans un délai raisonnable et, avant de faire à nouveau usage de la dérogation, fournissent les éléments prouvant que le taux de fraude qu'ils contrôlent est redevenu conforme au taux de référence en matière de fraude applicable pour cette fourchette de seuils de dérogation conformément au paragraphe 3 du présent article.

Article 21
Contrôle

1. Pour faire usage des dérogations prévues aux articles 10 à 18, les prestataires de services de paiement enregistrent et contrôlent les données suivantes pour chaque type d'opérations de paiement, en les ventilant par opérations à distance et autres opérations, au moins sur une base trimestrielle:

   (a) la valeur totale des opérations de paiement non autorisées ou frauduleuses, conformément à l'article 64, paragraphe 2, de la directive (UE) 2015/2366, la valeur totale de l'ensemble des opérations de paiement et le taux de fraude qui en découle, comprenant une ventilation par opérations de paiement initiées grâce à l'authentification forte du client et au titre de chacune des dérogations;

   (b) la valeur moyenne des opérations, comprenant une ventilation par opérations de paiement initiées grâce à l'authentification forte du client et au titre de chacune des dérogations;

   (c) le nombre d'opérations de paiement pour lesquelles chacune des dérogations a été appliquée et le pourcentage qu'elles représentent par rapport au nombre total d'opérations de paiement.

2. Les prestataires de services de paiement mettent les résultats du contrôle effectué conformément au paragraphe 1 à la disposition des autorités compétentes et de l'ABE, moyennant une notification préalable à l'(aux) autorité(s) compétente(s) correspondante(s), à leur demande.

CHAPITRE IV
CONFIDENTIALITÉ ET INTÉGRITÉ DES DONNÉES DE SÉCURITÉ PERSONNALISÉES DES UTILISATEURS DE SERVICES DE PAIEMENT

Article 22
Exigences générales

1. Les prestataires de services de paiement veillent à la confidentialité et à l'intégrité des données de sécurité personnalisées de l'utilisateur de services de paiement, notamment des codes d'authentification, durant l'ensemble des phases de l'authentification.

2. Aux fins du paragraphe 1, les prestataires de services de paiement garantissent le respect de chacune des exigences suivantes:

   (a) les données de sécurité personnalisées sont masquées lorsqu'elles sont affichées et ne sont pas lisibles dans leur intégralité lorsqu'elles sont entrées par l'utilisateur de services de paiement durant l'authentification;

   (b) les données de sécurité personnalisées en format de données ainsi que le matériel cryptographique lié au cryptage des données de sécurité personnalisées ne sont pas conservés en texte clair;

   (c) le matériel cryptographique secret est protégé de toute divulgation non autorisée.

3. Les prestataires de services de paiement consignent intégralement par écrit le processus de gestion du matériel cryptographique utilisé pour crypter ou rendre illisibles d'une autre manière les données de sécurité personnalisées.

4. Les prestataires de services de paiement veillent à ce que le traitement et le routage des données de sécurité personnalisées et des codes d'authentification générés conformément au chapitre II aient lieu dans des environnements sécurisés suivant des normes sectorielles rigoureuses et largement reconnues.

Article 23
Création et transmission des données

Les prestataires de services de paiement veillent à ce que la création des données de sécurité personnalisées ait lieu dans un environnement sécurisé.

Ils réduisent les risques d'utilisation non autorisée des données de sécurité personnalisées ainsi que des dispositifs et du logiciel d'authentification à la suite de leur perte, vol ou copie avant leur livraison au payeur.

Article 24
Association avec l'utilisateur de services de paiement

1. Les prestataires de services de paiement veillent à ce que seul l'utilisateur de services de paiement soit associé, de manière sécurisée, aux données de sécurité personnalisées, aux dispositifs d'authentification et au logiciel.

2. Aux fins du paragraphe 1, les prestataires de services de paiement garantissent le respect de chacune des exigences suivantes:

(a) l’association de l’identité de l’utilisateur de services de paiement avec les données de sécurité personnalisées et les dispositifs et le logiciel d’authentification a lieu dans des environnements sécurisés relevant de la responsabilité du prestataire de services de paiement, comprenant au moins les locaux du prestataire de services de paiement et l’environnement internet fourni par le prestataire de services de paiement, ou d’autres sites internet sécurisés similaires utilisés par ce dernier et par ses services de retrait à des distributeurs automatiques de billets, et tenant compte des risques liés aux dispositifs et composants sous-jacents utilisés au cours du processus d’association qui ne sont pas sous la responsabilité du prestataire de services de paiement;

(b) l’association, grâce à un moyen de communication à distance, de l’identité de l’utilisateur de services de paiement avec les données de sécurité personnalisées et les dispositifs ou le logiciel d’authentification est effectuée à l’aide d'une authentification forte du client.

Article 25

Livraison des données ainsi que des dispositifs et du logiciel d’authentification

1. Les prestataires de services de paiement veillent à ce que la livraison des données de sécurité personnalisées ainsi que des dispositifs et du logiciel d’authentification à l’utilisateur de services de paiement soit effectuée d’une manière sécurisée qui permette de prévenir les risques liés à leur utilisation non autorisée à la suite de leur perte, vol ou copie.

2. Aux fins du paragraphe 1, les prestataires de services de paiement appliquent au moins chacune des mesures suivantes:

(a) des mécanismes de livraison efficaces et sécurisés garantissent que les données de sécurité personnalisées ainsi que les dispositifs et le logiciel d’authentification sont livrés à l’utilisateur de services de paiement légitime;

(b) des mécanismes permettent au prestataire de services de paiement de vérifier l’authenticité du logiciel d’authentification livré à l’utilisateur de services de paiement grâce à l’internet;

(c) des dispositions garantissent que, lorsque la livraison des données de sécurité personnalisées a lieu en dehors des locaux du prestataire de services de paiement ou grâce à un moyen de communication à distance:

i) aucun tiers non autorisé ne peut obtenir plus d’un élément des données de sécurité personnalisées ou des dispositifs ou du logiciel d’authentification lorsque la livraison est effectuée grâce au même moyen de communication;

ii) les données de sécurité personnalisées ou les dispositifs ou le logiciel d’authentification doivent être activés avant de pouvoir être utilisés;

(d) des dispositions garantissent que, si les données de sécurité personnalisées ou les dispositifs ou le logiciel d’authentification doivent être activés avant leur première utilisation, cette activation est effectuée dans un environnement sécurisé conformément aux procédures d’association visées à l’article 24.

Article 26
Renouvellement des données de sécurité personnalisées

Les prestataires de services de paiement veillent à ce que le renouvellement ou la réactivation des données de sécurité personnalisées respecte les procédures applicables à la création, l'association et la livraison de ces données et des dispositifs d'authentification conformément aux articles 23, 24 et 25.

Article 27
Destruction, désactivation et révocation

Les prestataires de services de paiement veillent à mettre en place des procédures efficaces en vue d'appliquer chacune des mesures de sécurité suivantes:

(a) la destruction, la désactivation ou la révocation sécurisée des données de sécurité personnalisées et des dispositifs et du logiciel d'authentification;

(b) lorsque le prestataire de services de paiement distribue des dispositifs et logiciels d'authentification réutilisables, la réutilisation sécurisée d'un dispositif ou logiciel est établie, décrite par écrit et mise en œuvre avant sa mise à disposition d'un autre utilisateur de services de paiement;

(c) la désactivation ou la révocation des informations liées aux données de sécurité personnalisées conservées dans les systèmes et bases de données du prestataire de services de paiement et, le cas échéant, dans des registres publics.

CHAPITRE V
NORMES OUVERTES COMMUNES ET SÉCURISÉES DE COMMUNICATION

SECTION 1
EXIGENCES GENERALES RELATIVES A LA COMMUNICATION

Article 28
Exigences relatives à l'identification

1. Les prestataires de services de paiement garantissent une identification sécurisée lors des communications entre le dispositif du payeur et les dispositifs du bénéficiaire visant à accepter les paiements électroniques, notamment, mais pas exclusivement, les terminaux de paiement.

2. Les prestataires de services de paiement veillent à ce que les risques que la communication soit déviée vers des tiers non autorisés dans le cadre d'applications mobiles, ou d'autres interfaces pour utilisateurs de services de paiement, proposant des services de paiement électronique soient efficacement réduits.

Article 29
Traçabilité

1. Les prestataires de services de paiement mettent en place des procédures qui garantissent que l'ensemble des opérations de paiement et des autres interactions avec l'utilisateur de services de paiement, avec d'autres prestataires de services de paiement et avec d'autres entités, y compris des commerçants, dans le cadre de la

prestation du service de paiement, sont traçables, afin que l'ensemble des événements en rapport avec l'opération électronique durant ses différentes phases soient connus a posteriori.

2. Aux fins du paragraphe 1, les prestataires de services de paiement veillent à ce que toute session de communication avec l'utilisateur de services de paiement, d'autres prestataires de services de paiement et d'autres entités, y compris des commerçants, s'appuie sur chacun des éléments suivants:

(a) un identifiant unique de la session;

(b) des mécanismes de sécurité pour l'enregistrement détaillé de l'opération, y compris le numéro de l'opération, les horodatages et toutes les données pertinentes de l'opération;

(c) des horodatages qui sont fondés sur un système unifié de représentation du temps et qui sont synchronisés conformément à un signal horaire officiel.

SECTION 2
EXIGENCES SPECIFIQUES RELATIVES AUX NORMES OUVERTES COMMUNES ET SECURISEES DE COMMUNICATION

Article 30
Obligations générales relatives aux interfaces d'accès

1. Un prestataire de services de paiement gestionnaires de comptes qui propose à un payeur un compte de paiement accessible en ligne met en place au moins une interface qui remplit chacune des exigences suivantes:

(a) les prestataires de services d'information sur les comptes, les prestataires de services d'initiation de paiement et les prestataires de services de paiement qui émettent des instruments de paiement liés à une carte sont en mesure de s'identifier auprès du prestataire de services de paiement gestionnaire du compte;

(b) les prestataires de services d'information sur les comptes sont en mesure de communiquer de manière sécurisée afin de demander et de recevoir des informations concernant un ou plusieurs comptes de paiement désignés et les opérations de paiement associées;

(c) les prestataires de services d'initiation de paiement sont en mesure de communiquer de manière sécurisée pour initier un ordre de paiement à partir du compte de paiement du payeur et de recevoir toutes les informations sur l'initiation de l'opération de paiement et toutes les informations auxquelles le prestataire de services de paiement gestionnaire du compte a accès concernant l'exécution de l'opération de paiement.

2. Aux fins de l'authentification de l'utilisateur de services de paiement, l'interface visée au paragraphe 1 permet aux prestataires de services d'information sur les comptes et aux prestataires de services d'initiation de paiement de s'appuyer sur l'ensemble des procédures d'authentification proposées par le prestataire de services de paiement gestionnaire du compte à l'utilisateur de services de paiement.

L'interface remplit au moins l'ensemble des exigences suivantes:

(a) un prestataire de services d'initiation de paiement ou un prestataire de services d'information sur les comptes est en mesure de donner instruction au prestataire de services de paiement gestionnaire du compte de commencer l'authentification sur la base du consentement de l'utilisateur de services de paiement;

(b) les sessions de communication entre le prestataire de services de paiement gestionnaire du compte, le prestataire de services d'information sur les comptes, le prestataire de services d'initiation de paiement et tout utilisateur de services de paiement concerné sont établies et maintenues tout au long de l'authentification;

(c) l'intégrité et la confidentialité des données de sécurité personnalisées et des codes d'authentification transmis par ou via le prestataire de services d'initiation de paiement ou le prestataire de services d'information sur les comptes sont garanties.

3. Les prestataires de services de paiement gestionnaires de comptes veillent à ce que leurs interfaces suivent des normes de communication publiées par des organisations européennes ou internationales de normalisation.

Les prestataires de services de paiement gestionnaires de comptes veillent également à ce que les spécifications techniques des interfaces fassent l'objet d'une documentation mentionnant une série de routines, de protocoles et d'outils dont les prestataires de services d'initiation de paiement, les prestataires de services d'information sur les comptes et les prestataires de services de paiement qui émettent des instruments de paiement liés à une carte ont besoin pour permettre l'interopérabilité de leurs logiciels et applications avec les systèmes des prestataires de services de paiement gestionnaires de comptes.

Au minimum, les prestataires de services de paiement gestionnaires de comptes, au moins six mois avant la date d'application visée à l'article 38, paragraphe 2, ou avant la date prévue pour le lancement sur le marché de l'interface d'accès lorsque ce lancement a lieu après la date visée à l'article 38, paragraphe 2, mettent gratuitement à disposition cette documentation à la demande des prestataires agréés de services d'initiation de paiement, de services d'information sur les comptes et de services de paiement qui émettent des instruments de paiement liés à une carte ou des prestataires de services de paiement qui ont demandé l'agrément nécessaire à leurs autorités compétentes, et publient sur leur site internet un résumé de cette documentation.

4. Outre les dispositions prévues au paragraphe 3, les prestataires de services de paiement gestionnaires de comptes veillent à ce que, sauf en cas d'urgence, toute modification des spécifications techniques de leur interface soit mise à la disposition des prestataires agréés de services d'initiation de paiement, de services d'information sur les comptes et de services de paiement qui émettent des instruments de paiement liés à une carte ou des prestataires de services de paiement qui ont demandé l'agrément nécessaire à leurs autorités compétentes, dans les plus brefs délais et au moins trois mois avant la mise en œuvre de la modification.

Les prestataires de services de paiement décrivent par écrit les situations d'urgence dans lesquelles les modifications ont été mises en œuvre et mettent cette documentation à la disposition des autorités compétentes sur demande.

5. Les prestataires de services de paiement gestionnaires de comptes mettent à disposition un dispositif d'essai, comprenant une assistance et permettant des tests de connexion et de fonctionnement, afin que les prestataires agréés de services

d'initiation de paiement, de services de paiement qui émettent des instruments de paiement liés à une carte et de services d'information sur les comptes ou les prestataires de services de paiement qui ont demandé l'agrément nécessaire puissent tester les logiciels et applications qu'ils utilisent pour proposer un service de paiement aux utilisateurs. Il convient que ce dispositif d'essai soit mis à disposition au moins six mois avant la date d'application visée à l'article 38, paragraphe 2, ou avant la date prévue pour le lancement sur le marché de l'interface d'accès lorsque ce lancement a lieu après la date visée à l'article 38, paragraphe 2.

Aucune information sensible n'est toutefois partagée par l'intermédiaire du dispositif d'essai.

6. Les autorités compétentes veillent à ce que les prestataires de services de paiement gestionnaires de comptes respectent à tout moment les obligations prévues par les présentes normes en ce qui concerne l'(les) interface(s) qu'ils ont mise(s) en place. Si un prestataire de services de paiement gestionnaire de comptes ne remplit pas les exigences relatives aux interfaces définies par les présentes normes, les autorités compétentes veillent à ce que la prestation des services d'initiation de paiement et des services d'information sur les comptes ne soit pas empêchée ou perturbée, dans la mesure où les prestataires respectifs de ces services satisfont aux conditions définies à l'article 33, paragraphe 5.

Article 31
Options des interfaces d'accès

Les prestataires de services de paiement gestionnaires de comptes établissent l'(les) interface(s) visée(s) à l'article 30 en mettant en place une interface dédiée ou en permettant l'utilisation par les prestataires de services de paiement visés à l'article 30, paragraphe 1, des interfaces servant à l'authentification et à la communication avec les utilisateurs de services de paiement des prestataires de services de paiement gestionnaires de comptes.

Article 32
Obligations applicables à une interface dédiée

1. Sous réserve du respect des articles 30 et 31, les prestataires de services de paiement gestionnaires de comptes qui ont mis en place une interface dédiée veillent à ce que celle-ci offre à tout moment le même niveau de disponibilité et de performances, assistance comprise, que les interfaces mises à la disposition de l'utilisateur de services de paiement pour accéder directement à son compte de paiement en ligne.

2. Les prestataires de services de paiement gestionnaires de comptes qui ont mis en place une interface dédiée définissent des indicateurs de performance clés et des valeurs cibles de niveau de service qui soient transparents et au moins aussi exigeants que ceux fixés pour l'interface utilisée par leurs utilisateurs de services de paiement, tant sur le plan de la disponibilité que des données fournies conformément à l'article 36. Ces interfaces, indicateurs et valeurs cibles sont contrôlés par les autorités compétentes et soumis à un test de résistance.

3. Les prestataires de services de paiement gestionnaires de comptes qui ont mis en place une interface dédiée veillent à ce que cette interface n'entrave pas la prestation de services d'initiation de paiement et d'information sur les comptes. Les entraves peuvent consister notamment à empêcher l'utilisation par les prestataires de services de paiement visés à l'article 30, paragraphe 1, des données de sécurité émises par les

prestataires de services de paiement gestionnaires de comptes à l'intention de leurs clients, à imposer la redirection vers l'authentification ou d'autres fonctions du prestataire de services de paiement gestionnaire du compte, à exiger des agréments et enregistrements en plus de ceux prévus aux articles 11, 14 et 15 de la directive 2015/2366 ou à demander des contrôles supplémentaires du consentement donné par les utilisateurs de services de paiement aux prestataires de services d'initiation de paiement et d'information sur les comptes.

4. Aux fins des paragraphes 1 et 2, les prestataires de services de paiement gestionnaires de comptes contrôlent la disponibilité et les performances de l'interface dédiée. Les prestataires de services de paiement gestionnaires de comptes publient sur leur site internet des statistiques trimestrielles concernant la disponibilité et les performances de l'interface dédiée et de l'interface utilisée par leurs utilisateurs de services de paiement.

Article 33

Mesures d'urgence applicables à une interface dédiée

1. Les prestataires de services de paiement gestionnaires de comptes prévoient, lors de la conception de l'interface dédiée, une stratégie et des plans relatifs à des mesures d'urgence, au cas où l'interface ne fonctionnerait pas conformément à l'article 32, où elle serait indisponible de façon imprévue et où le système tomberait en panne. Une indisponibilité imprévue ou une panne du système peut être présumée lorsque cinq demandes consécutives d'accès aux informations pour la prestation de services d'initiation de paiement ou de services d'information sur les comptes n'obtiennent pas de réponse dans les 30 secondes.

2. Les mesures d'urgence comprennent des plans de communication visant à informer les prestataires de services de paiement qui utilisent l'interface dédiée des mesures destinées à restaurer le système, ainsi qu'une description des autres options immédiatement disponibles dont les prestataires de services de paiement peuvent faire usage pendant ce temps.

3. Le prestataire de services de paiement gestionnaire du compte et les prestataires de services de paiement visés à l'article 30, paragraphe 1, notifient sans délai les problèmes liés aux interfaces dédiées décrits au paragraphe 1 à leurs autorités compétentes nationales respectives.

4. Dans le cadre d'un mécanisme d'urgence, les prestataires de services de paiement visés à l'article 30, paragraphe 1, sont autorisés à utiliser les interfaces mises à la disposition des utilisateurs de services de paiement en vue de l'authentification et de la communication avec leur prestataire de services de paiement gestionnaire de comptes, jusqu'à ce que l'interface dédiée retrouve le niveau de disponibilité et de performances prévu à l'article 32.

5. À cet effet, les prestataires de services de paiement gestionnaires de comptes veillent à ce que les prestataires de services de paiement visés à l'article 30, paragraphe 1, puissent être identifiés et s'appuyer sur les procédures d'authentification proposées par le prestataire de services de paiement gestionnaire du compte à l'utilisateur de services de paiement. Lorsqu'ils utilisent l'interface visée au paragraphe 4, les prestataires de services de paiement visés à l'article 30, paragraphe 1:

(a) prennent les mesures nécessaires pour garantir qu'ils n'accèdent pas à des données ou qu'ils ne conservent ou ne traitent pas de données à des fins autres que la prestation du service demandé par l'utilisateur de services de paiement;

(b) continuent à se conformer aux obligations découlant respectivement de l'article 66, paragraphe 3, et de l'article 67, paragraphe 2, de la directive (UE) 2015/2366;

(c) enregistrent les données auxquelles ils ont accès par l'intermédiaire de l'interface exploitée par le prestataire de services de paiement gestionnaire de comptes pour ses utilisateurs de services de paiement et fournissent ce registre, sur demande et sans retard injustifié, à leur autorité nationale compétente;

(d) justifient dûment auprès de leur autorité nationale compétente, sur demande et sans retard injustifié, l'utilisation de l'interface mise à la disposition des utilisateurs de services de paiement pour accéder directement à leur compte de paiement en ligne;

(e) informent en conséquence le prestataire de services de paiement gestionnaire du compte.

6. Les autorités compétentes, après avoir consulté l'ABE pour assurer l'application cohérente des conditions suivantes, exemptent les prestataires de services de paiement gestionnaires de comptes qui ont choisi une interface dédiée de l'obligation de mettre en place le mécanisme d'urgence décrit au paragraphe 4 lorsque l'interface dédiée remplit l'ensemble des conditions suivantes:

(a) elle est conforme à l'ensemble des obligations applicables aux interfaces dédiées, telles qu'énoncées à l'article 32;

(b) elle a été conçue et testée conformément à l'article 30, paragraphe 5, à la satisfaction des prestataires de services de paiement qui y sont mentionnés;

(c) elle a été largement utilisée pendant au moins trois mois par des prestataires de services de paiement en vue de proposer des services d'information sur les comptes et des services d'initiation de paiement et de confirmer la disponibilité des fonds pour des paiements liés à une carte;

(d) tout problème lié à l'interface dédiée a été résolu sans retard injustifié.

7. Les autorités compétentes annulent la dérogation visée au paragraphe 6 lorsque les conditions a) et d) ne sont pas remplies par les prestataires de services de paiement gestionnaires de comptes pendant plus de deux semaines civiles consécutives. Elles informent l'ABE de cette annulation et veillent à ce que le prestataire de services de paiement gestionnaire de comptes mette en place, dans les plus brefs délais et au plus tard dans les deux mois, le mécanisme d'urgence visé au paragraphe 4.

Article 34
Certificats

1. Aux fins de l'identification visée à l'article 30, paragraphe 1, point a), les prestataires de services de paiement ont recours à des certificats qualifiés de cachet électronique tels que mentionnés à l'article 3, point 30, du règlement (UE) nº 910/2014 du

Parlement européen et du Conseil ou à des certificats qualifiés d'authentification de site internet, tels que prévus à l'article 3, point 39, dudit règlement.

2. Aux fins du présent règlement, le numéro d'immatriculation tel que mentionné dans les registres officiels conformément à l'annexe III, point c), ou à l'annexe IV, point c), du règlement (UE) nº 910/2014 est le numéro d'agrément des prestataires de services de paiement qui émettent des instruments de paiement liés à une carte, des prestataires de services d'information sur les comptes et des prestataires de services d'initiation de paiement (y compris des prestataires de services de paiement gestionnaires de comptes fournissant ces services), disponible dans le registre public de l'État membre d'origine conformément à l'article 14 de la directive (UE) 2015/2366 ou découlant de la notification, conformément à l'article 20 de la directive 2013/36/UE du Parlement européen et du Conseil[4], de chaque agrément octroyé en vertu de l'article 8 de cette directive.

3. Aux fins du présent règlement, les certificats qualifiés de cachet électronique ou d'authentification de site internet visés au paragraphe 1 contiennent, dans une langue usuelle dans la sphère financière internationale, des attributs spécifiques supplémentaires concernant chacun des éléments suivants:

(a) le rôle du prestataire de services de paiement, qui peut consister en une ou plusieurs des fonctions suivantes:

i) la gestion de comptes;

ii) l'initiation de paiements;

iii) l'information sur les comptes;

iv) l'émission d'instruments de paiement liés à une carte;

(b) le nom des autorités compétentes auprès desquelles le prestataire de services de paiement est enregistré.

4. Les attributs visés au paragraphe 3 n'ont pas d'incidence sur l'interopérabilité et la reconnaissance des certificats qualifiés de cachet électronique ou d'authentification de site internet.

Article 35
Sécurité des sessions de communication

1. Les prestataires de services de paiement gestionnaires de comptes, les prestataires de services de paiement qui émettent des instruments de paiement liés à une carte, les prestataires de services d'information sur les comptes et les prestataires de services d'initiation de paiement veillent à ce que, lors de l'échange de données par l'internet, un cryptage sécurisé soit utilisé entre les parties communicantes tout au long de la session de communication concernée afin de préserver la confidentialité et l'intégrité des données, à l'aide de techniques de cryptage performantes et largement reconnues.

2. Les prestataires de services de paiement qui émettent des instruments de paiement liés à une carte, les prestataires de services d'information sur les comptes et les

[4] Directive 2013/36/UE du Parlement européen et du Conseil du 26 juin 2013 concernant l'accès à l'activité des établissements de crédit et la surveillance prudentielle des établissements de crédit et des entreprises d'investissement, modifiant la directive 2002/87/CE et abrogeant les directives 2006/48/CE et 2006/49/CE (JO L 176 du 27.6.2013, p. 338).

prestataires de services d'initiation de paiement font en sorte que les sessions d'accès proposées par les prestataires de services de paiement gestionnaires de comptes soient aussi brèves que possible et mettent activement fin à toute session de ce type dès que l'action demandée a été menée à bien.

3. Lorsqu'ils maintiennent des sessions de réseau parallèles avec le prestataire de services de paiement gestionnaire du compte, les prestataires de services d'information sur les comptes et les prestataires de services d'initiation de paiement veillent à ce que ces sessions soient liées de manière sécurisée aux sessions correspondantes établies avec l'utilisateur ou les utilisateurs de services de paiement, afin d'éviter que des messages ou des informations qu'ils se communiquent puissent être détournés.

4. Les prestataires de services d'information sur les comptes, les prestataires de services d'initiation de paiement et les prestataires de services de paiement qui émettent des instruments de paiement liés à une carte avec le prestataire de services de paiement gestionnaire du compte indiquent des références claires à chacun des éléments suivants:

(a) l'utilisateur ou les utilisateurs de services de paiement et la session de communication correspondante, afin d'opérer une distinction entre plusieurs demandes émanant du (des) même(s) utilisateur(s) de services de paiement;

(b) pour les services d'initiation de paiement, l'opération de paiement initiée, identifiée de manière unique;

(c) pour la confirmation de la disponibilité des fonds, la demande identifiée de manière unique portant sur le montant nécessaire pour l'exécution de l'opération de paiement liée à une carte.

5. Les prestataires de services de paiement gestionnaires de comptes, les prestataires de services d'information sur les comptes, les prestataires d'initiation de paiement et les prestataires de services de paiement qui émettent des instruments de paiement liés à une carte veillent à ce que, lorsqu'ils communiquent des données de sécurité personnalisées et des codes d'authentification, ceux-ci ne soient à aucun moment lisibles, directement ou indirectement, par un membre du personnel.

En cas de perte de confidentialité des données de sécurité personnalisées relevant de leur compétence, ces prestataires informent sans délai l'utilisateur de services de paiement qui leur est associé, ainsi que l'émetteur des données de sécurité personnalisées.

Article 36
Échanges de données

1. Les prestataires de services de paiement gestionnaires de comptes remplissent chacune des exigences suivantes:

(a) ils fournissent aux prestataires de services d'information sur les comptes les mêmes informations provenant des comptes de paiement désignés et des opérations de paiement associées que celles qui sont mises à la disposition de l'utilisateur de services de paiement en cas de demande directe d'accès aux informations sur le compte, pour autant que ces informations ne comportent pas de données de paiement sensibles;

(b) immédiatement après avoir reçu l'ordre de paiement, ils fournissent aux prestataires de services d'initiation de paiement les mêmes informations sur l'initiation et l'exécution de l'opération de paiement que celles qui sont fournies ou mises à la disposition de l'utilisateur de services de paiement lorsque ce dernier initie directement l'opération;

(c) sur demande, ils fournissent immédiatement aux prestataires de services de paiement la confirmation, sous la forme d'un simple «oui» ou «non», que le montant nécessaire à l'exécution d'une opération de paiement est disponible ou non sur le compte de paiement du payeur.

2. En cas d'erreur ou d'événement imprévu au cours de la procédure d'identification ou d'authentification ou lors de l'échange d'éléments d'information, le prestataire de services de paiement gestionnaire du compte envoie un message de notification au prestataire de services d'initiation de paiement ou au prestataire de services d'information sur les comptes et au prestataire de services de paiement qui émet des instruments de paiement liés à une carte, en indiquant les raisons de l'erreur ou de l'événement imprévu.

Lorsque le prestataire de services de paiement gestionnaire du compte propose une interface dédiée conformément à l'article 32, l'interface prévoit que des messages de notification des erreurs ou événements imprévus soient transmis par tout prestataire de services de paiement qui décèle l'événement ou l'erreur aux autres prestataires de services de paiement participant à la session de communication.

3. Les prestataires de services d'information sur les comptes mettent en place des mécanismes appropriés et efficaces qui empêchent l'accès à d'autres informations que celles provenant des comptes de paiement désignés et des opérations de paiement associées, conformément au consentement explicite de l'utilisateur.

4. Les prestataires de services d'initiation de paiement fournissent aux prestataires de services de paiement gestionnaires de comptes les mêmes informations que celles qui sont demandées à l'utilisateur de services de paiement lors de l'initiation directe de l'opération de paiement.

5. Les prestataires de services d'information sur les comptes sont en mesure d'accéder aux informations provenant des comptes de paiement désignés et des opérations de paiement associées qui sont détenues par les prestataires de services de paiement gestionnaires de comptes aux fins de la prestation des services d'information sur les comptes dans l'une des situations suivantes:

(a) chaque fois que l'utilisateur de services de paiement demande spontanément ces informations;

(b) si l'utilisateur de services de paiement ne demande pas spontanément ces informations, au maximum quatre fois par période de 24 heures, sauf si une fréquence plus élevée est convenue entre le prestataire de services d'information sur les comptes et le prestataire de services de paiement gestionnaire du compte, avec le consentement de l'utilisateur de services de paiement.

CHAPITRE VI
DISPOSITIONS FINALES

Article 37
Réexamen

Sans préjudice de l'article 98, paragraphe 5, de la directive (UE) 2015/2366, l'ABE réexamine pour le [*OP: veuillez insérer la date correspondant à 18 mois après la date d'application visée à l'article 38, paragraphe 2*] les taux de fraude visés à l'annexe du présent règlement, ainsi que les dérogations octroyées au titre de l'article 33, paragraphe 6, concernant les interfaces dédiées et, le cas échéant, soumet à la Commission les projets de mise à jour de celles-ci, conformément à l'article 10 du règlement (UE) nº 1093/2010.

Article 38
Entrée en vigueur

1. Le présent règlement entre en vigueur le jour suivant celui de sa publication au *Journal officiel de l'Union européenne*.
2. Le présent règlement s'applique à partir du [OP: veuillez insérer la date correspondant à 18 mois après la date d'entrée en vigueur].
3. Toutefois, l'article 30, paragraphes 3 et 5, s'applique à partir du [OP: veuillez insérer la date correspondant à 12 mois après la date d'entrée en vigueur].

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

Fait à Bruxelles, le 27.11.2017

Par la Commission
Le président,
Jean-Claude JUNCKER