

En cas de divergences entre les textes français et anglais, le texte anglais prévaut.

Luxembourg, le 14 mars 2019

À tous les prestataires de services de
paiement

CIRCULAIRE CSSF 19/712

Concerne : Orientations de l'Autorité bancaire européenne concernant les exigences pour la déclaration de données relatives à la fraude au titre de l'article 96, paragraphe 6, de la directive (UE) 2015/2366 (PSD2) (EBA/GL/2018/05)

Mesdames, Messieurs,

L'objet de la présente circulaire est de porter à votre attention les Orientations de l'Autorité bancaire européenne (« **EBA** ») concernant les exigences pour la déclaration de données relatives à la fraude au titre de l'article 96, paragraphe 6, de la directive (UE) 2015/2366 (« **PSD2** »)¹ - EBA/GL/2018/05 (les « **Orientations** ») que la CSSF entend respecter en sa capacité d'autorité compétente.

Les Orientations fournissent des précisions sur les obligations de déclaration des données relatives à la fraude comme le prévoit l'article 105-3, paragraphe 3, de la loi modifiée du 10 novembre 2009 relative aux services de paiement² (la « **Loi** »).

1. Les Orientations

Les Orientations fournissent des précisions sur les données statistiques relatives à la fraude liée aux différents moyens de paiement que les prestataires de services de paiement (tels que définis ci-dessous) doivent communiquer à leurs autorités compétentes, ainsi que sur les données agrégées que les autorités compétentes doivent communiquer à l'EBA et à la Banque centrale européenne, conformément à l'article 96, paragraphe 6, de la directive PSD2. Les Orientations définissent les différents types d'opérations de paiement et les opérations de paiement frauduleuses à communiquer ainsi que la fréquence, les délais et les périodes de déclaration.

¹ 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) n° 1093/2010, et abrogeant la directive 2007/64/CE

² Loi du 10 novembre 2009 relative aux services de paiement, à l'activité d'établissement de monnaie électronique et au caractère définitif du règlement dans les systèmes de paiement et les systèmes de règlement des opérations sur titres

2. Champ d'application

La présente circulaire s'adresse aux prestataires de services de paiement tels que définis à l'article 1, point 37), de la Loi, pour lesquels la CSSF est l'autorité compétente désignée à des fins de surveillance (« PSP »), à l'exception des prestataires de services d'information sur les comptes tels que définis à l'article 1, point 37quinquies), de la Loi.

3. Périodes de déclaration, délais et détails techniques

Un PSP doit déclarer les données tous les six mois en respectant la(les) ventilation(s) indiquée(s) en annexe 2 des Orientations. Les instructions techniques détaillées concernant l'envoi des données statistiques relatives à la fraude telles que prévues à l'article 105-2, paragraphe 3, de la Loi seront publiées séparément sur le site de la CSSF à un stade ultérieur.

Les données déclarées devront être soumises à la CSSF dans les trois mois suivant la fin de la période de déclaration. Les deux périodes semestrielles de déclaration sont les suivantes : entre le 1^{er} janvier et le 30 juin, respectivement entre le 1^{er} juillet et le 31 décembre. La première déclaration devra être présentée au plus tard le 30 septembre 2020. La déclaration de fraude est à faire même s'il n'y a pas eu de fraude durant la période de déclaration.

4. Ajustements par rapport aux données déclarées dans le passé

Les PSP devraient déclarer tous les ajustements apportés aux données relatives à une période de déclaration passée durant de la prochaine période de déclaration une fois que les informations à ajuster ont été identifiées, en soumettant les tableaux de déclaration révisés respectifs et en indiquant la période de déclaration passée à laquelle ils se réfèrent selon les instructions techniques détaillées mentionnées à la section 3.

5. Date d'application

La présente circulaire s'applique à compter du 1^{er} janvier 2020.

Les Orientations sont annexées à la présente circulaire et elles sont disponibles sur le site Internet de l'EBA à l'adresse :

<https://eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-fraud-reporting-under-psd2>.

Veillez recevoir, Mesdames, Messieurs, l'assurance de nos sentiments distingués.

COMMISSION de SURVEILLANCE du SECTEUR FINANCIER

Marco ZWICK

Directeur

Claude WAMPACH

Directeur

Jean-Pierre FABER

Directeur

Françoise KAUTHEN

Directeur

Claude MARX

Directeur général

EBA/GL/2018/05

17/09/2018

Orientations

concernant les exigences pour la
déclaration de données relatives à la
fraude au titre de l'article 96,
paragraphe 6, de la DSP2



1. Obligations de conformité et de déclaration

Statut de ces orientations

1. Le présent document contient des orientations émises en vertu de l'article 16 du règlement (UE) n° 1093/2010¹. Conformément à l'article 16, paragraphe 3, du règlement (UE) n° 1093/2010, les autorités compétentes et les établissements financiers mettent tout en œuvre pour respecter ces orientations.
2. Les orientations donnent l'avis de l'ABE sur des pratiques de surveillance appropriées au sein du système européen de surveillance financière ou sur les modalités d'application du droit de l'Union dans un domaine particulier. Les autorités compétentes, telles que définies à l'article 4, paragraphe 2, du règlement (UE) n° 1093/2010, qui sont soumises aux orientations, doivent les respecter en les intégrant dans leurs pratiques, s'il y a lieu (par exemple en modifiant leur cadre juridique ou leurs processus de surveillance), y compris lorsque les orientations s'adressent principalement à des établissements.

Obligations de déclaration

3. Conformément à l'article 16, paragraphe 3, du règlement (UE) n° 1093/2010, les autorités compétentes doivent indiquer à l'ABE si elles respectent ou entendent respecter ces orientations, ou indiquer les raisons du non-respect des orientations, le cas échéant, avant le 19.11.2018. En l'absence d'une notification avant cette date, les autorités compétentes seront considérées par l'ABE comme n'ayant pas respecté les orientations. Les notifications sont à adresser à compliance@eba.europa.eu à l'aide du formulaire disponible sur le site internet de l'ABE et en indiquant en objet «EBA/GL/2018/05». Les notifications doivent être communiquées par des personnes dûment habilitées à rendre compte du respect des orientations au nom des autorités compétentes. Toute modification du statut de conformité avec les orientations doit être signalée à l'ABE.
4. Les notifications seront publiées sur le site internet de l'ABE, conformément à l'article 16, paragraphe 3.

¹ Règlement (UE) n° 1093/2010 du Parlement européen et du Conseil du 24 novembre 2010 instituant une Autorité européenne de surveillance (l'Autorité bancaire européenne), modifiant la décision n° 716/2009/CE et abrogeant la décision 2009/78/CE de la Commission (JO L 331, 15.12.2010, p.12).

2. Objet, champ d'application et définitions

Objet

5. Les présentes orientations fournissent des précisions sur les données statistiques relatives aux différents moyens de paiement que les prestataires de services de paiement doivent communiquer à leurs autorités compétentes, ainsi que sur les données agrégées que les autorités compétentes doivent communiquer à l'ABE et à la BCE, conformément à l'article 96, paragraphe 6, de la directive (UE) 2015/2366 (DSP2).

Champ d'application

6. Les présentes orientations s'appliquent à la déclaration, par les prestataires de services de paiement aux autorités compétentes, des données statistiques concernant la fraude, pour les opérations de paiement initiées et exécutées (et acquises, le cas échéant), y compris pour l'acquisition d'opérations de paiement par carte, recensées par référence: a) aux données des opérations de paiement frauduleuses effectuées pendant une période déterminée et b) aux opérations de paiement effectuées au cours de la même période.
7. Les données déclarées dans le cadre de la ventilation des virements devraient inclure les virements effectués via des distributeurs automatiques de billets dotés d'une fonction de virement. Les virements utilisés pour régler les soldes d'opérations effectuées au moyen de cartes ayant une fonction de crédit ou de débit différé doivent également être inclus.
8. Les données déclarées dans le cadre de la ventilation des «prélèvements» devraient inclure les prélèvements utilisés pour régler le solde des opérations effectuées au moyen de cartes ayant une fonction de crédit ou de débit différé.
9. Les données déclarées au titre de la ventilation des paiements par carte devraient inclure les données sur l'ensemble des opérations de paiement effectuées au moyen de cartes de paiement (électroniques et non électroniques). Les paiements effectués par une carte dotée uniquement d'une fonction de «monnaie électronique» (par exemple les cartes prépayées) ne devraient pas être inclus dans les paiements par carte mais déclarés en tant que monnaie électronique.
10. Les présentes orientations précisent également comment les autorités compétentes devraient agréger les données mentionnées au paragraphe 6 qui doivent être communiquées à la BCE et à l'ABE en vertu de l'article 96, paragraphe 6, de la DSP2.
11. Les orientations sont soumises au principe de proportionnalité, ce qui signifie que tous les prestataires de services de paiement qui relèvent du champ d'application des orientations

doivent se conformer à chaque orientation, mais que les exigences précises, y compris en ce qui concerne la fréquence des déclarations, peuvent varier selon les prestataires de services de paiement en fonction de l'instrument de paiement utilisé, du type de service fourni et de la taille du prestataire de services de paiement.

Destinataires

12. Les présentes orientations sont destinées:

- aux prestataires de services de paiement tels que définis à l'article 4, paragraphe 11, de la directive (UE) 2015/2366 (DSP2) et visés dans la définition des «établissements financiers» figurant à l'article 4, paragraphe 1, du règlement (UE) n° 1093/2010, à l'exception des prestataires de services d'information sur les comptes, et
- aux autorités compétentes telles que définies à l'article 4, paragraphe 2, point i), du règlement (UE) n° 1093/2010.

Définitions

13. Sauf indication contraire, les termes utilisés et définis dans le règlement (UE) 2015/751 du Parlement européen et du Conseil du 29 avril 2015 relatif aux commissions d'interchange pour les opérations de paiement liées à une carte, dans le règlement (UE) n° 260/2012 du Parlement européen et du Conseil du Parlement européen et du Conseil du 14 mars 2012 établissant des exigences techniques et commerciales pour les virements et les prélèvements en euros, dans la directive (UE) 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur, et dans la directive 2009/110/CE du Parlement européen et du Conseil du 16 septembre 2009 concernant l'accès à l'activité des établissements de monnaie électronique et son exercice ainsi que la surveillance prudentielle de ces établissements, ont la même signification dans les présentes orientations.

Date d'entrée en vigueur

14. Les présentes orientations s'appliquent à compter du 1^{er} janvier 2019, à l'exception de la déclaration des données relatives aux dérogations à l'obligation d'utiliser l'authentification forte du client, telle que prévue dans le règlement délégué (UE) 2018/389 de la Commission complétant la directive (UE) 2015/2366 du Parlement européen et du Conseil par des normes techniques de réglementation relatives à l'authentification forte du client et à des normes ouvertes communes et sécurisées de communication, qui seront applicables à partir du 14 septembre 2019. ► A1 Les données relatives à ces dérogations sont détaillées à l'annexe 2, dans les ventilations des données A (de 1.3.1.2.4 à 1.3.1.2.9 et 1.3.2.2.4 à 1.3.2.2.8), C (3.2.1.3.4 à 3.2.1.3.10 et 3.2.2.3.4 à 3.2.2.3.8), D (4.2.1.3.4 à 4.2.1.3.8 et 4.2.2.3.4 à 4.2.2.3.7) et F (6.1.2.4 à 6.1.2.11 et 6.2.2.4 à 6.2.2.8).

3.1. Orientations sur la déclaration des données relatives à la fraude applicables aux prestataires de services de paiement

Orientation 1 Opérations de paiement et opérations de paiement frauduleuses

- 1.1 Aux fins de la déclaration des données statistiques relatives à la fraude, conformément aux présentes orientations, le prestataire de services de paiement devrait prendre en compte, pour chaque période de déclaration:
- a. toute opération de paiement non autorisée effectuée, y compris à la suite de la perte, du vol ou de l'appropriation illicite de données de paiement sensibles ou d'un instrument de paiement, qu'elle soit détectable ou non par le payeur avant un paiement et résultant ou non d'une négligence grave du payeur ou exécutée en l'absence de consentement du payeur («opération de paiement non autorisée»); et
 - b. toute opération de paiement effectuée à la suite d'une manipulation du payeur par le fraudeur, ayant pour effet d'émettre un ordre de paiement ou de donner instruction de le faire au prestataire de services de paiement, de bonne foi, à un compte de paiement qu'il estime appartenir à un bénéficiaire légitime («manipulation du payeur»).
- 1.2 Aux fins de l'orientation 1.1, le prestataire de services de paiement (y compris, le cas échéant, l'émetteur de l'instrument de paiement) ne devrait déclarer que les opérations de paiement qui ont été initiées et exécutées (et acquises le cas échéant). Le prestataire de services de paiement ne devrait pas déclarer les données relatives aux opérations de paiement qui, quel que soit leur lien avec l'une des situations visées dans l'orientation 1.1, n'ont pas été exécutées et n'ont pas entraîné de transfert de fonds conformément aux dispositions de la DSP2.
- 1.3 Dans le cas de services de transmission de fonds concernant des fonds transférés par le prestataire de services de paiement du payeur au prestataire de services de transmission de fonds du payeur (dans le cadre d'une opération de paiement de transmission de fonds), il appartient au prestataire de services de paiement du payeur, et non au prestataire de services de transmission de fonds du payeur, de déclarer les opérations de paiement effectuées par le prestataire de services de paiement du payeur en direction du prestataire de services de transmission de fonds. Ce type de transaction ne devrait pas être déclaré par

le prestataire de services de paiement du bénéficiaire de l'opération de paiement de transmission de fonds.

- 1.4 Les opérations et les opérations frauduleuses dans lesquelles des fonds ont été transférés par un prestataire de services de transmission de fonds, de ses comptes vers un compte bénéficiaire, y compris par des accords de compensation de la valeur d'opérations multiples (accords de compensation), devraient être déclarées par le prestataire de services de transmission de fonds conformément à la ventilation des données G de l'annexe 2.
- 1.5 Les opérations et les opérations frauduleuses dans lesquelles des fonds ont été transférés par un fournisseur de monnaie électronique vers un compte bénéficiaire, y compris lorsque le prestataire de services de paiement du payeur est le même que celui du bénéficiaire, devraient être déclarées par le fournisseur de monnaie électronique conformément à la ventilation des données F de l'annexe 2. Lorsque les prestataires de services de paiement sont différents, le paiement n'est déclaré que par le prestataire de services de paiement du payeur, afin d'éviter les doubles comptabilisations.
- 1.6 Les prestataires de services de paiement devraient déclarer l'ensemble des opérations de paiement et des opérations de paiement frauduleuses conformément aux dispositions suivantes:
 - a. Le «total des opérations de paiement frauduleuses» désigne l'ensemble des opérations visées dans l'orientation 1.1, que le montant de l'opération de paiement frauduleuse ait ou non été recouvré.
 - b. Les «pertes dues à une fraude, par porteur de responsabilité» désignent les pertes subies par le prestataire de services de paiement déclarant, son utilisateur de services de paiement ou d'autres intervenants, et reflètent l'incidence réelle de la fraude sur le plan des flux de trésorerie. Dans la mesure où l'enregistrement d'une perte financière subie peut être décalé dans le temps par rapport à la date réelle de l'opération frauduleuse, et afin d'éviter de devoir réviser les données communiquées au seul motif de ce décalage temporel inhérent, la perte définitive résultant d'une fraude devrait être déclarée au cours de la période durant laquelle elle est enregistrée dans les livres de compte du prestataire des services de paiement. Le montant définitif de la perte résultant d'une fraude ne devrait pas tenir compte des remboursements effectués par les organismes d'assurance, ces remboursements n'étant pas liés à la prévention de la fraude pour les besoins de la DSP2.
 - c. La «modification d'un ordre de paiement par le fraudeur» est une opération non autorisée telle que définie dans l'orientation 1.1, point a), et désigne une situation dans laquelle le fraudeur intercepte et modifie un ordre de paiement légitime à un moment donné de la communication électronique entre le dispositif du payeur et le prestataire de services de paiement [par exemple au moyen de logiciels malveillants ou d'attaques de type «man in the middle»] ou modifie l'instruction de paiement dans le système même du prestataire de services de paiement avant que l'ordre de paiement ne soit compensé et réglé.

- d. L'«émission d'un ordre de paiement par le fraudeur» est une opération non autorisée telle que définie dans l'orientation 1.1, point a), et désigne une situation dans laquelle un ordre de paiement factice est émis par un fraudeur qui a préalablement obtenu les données de paiement sensibles ou à caractère personnel du payeur/du bénéficiaire par des moyens frauduleux.

Orientation n° 2 Exigences générales concernant les données

- 2.1 Le prestataire de services de paiement devrait communiquer des informations statistiques sur:
 - a. l'ensemble des opérations de paiement, conformément aux différentes ventilations définies à l'annexe 2 et dans l'orientation 1; et
 - b. l'ensemble des opérations de paiement frauduleuses conformément aux différentes ventilations définies à l'annexe 2 et dans l'orientation 1.6, point a).
- 2.2 Le prestataire de services de paiement devrait déclarer les informations statistiques spécifiées dans l'orientation 2.1, tant en volume (nombre d'opérations ou d'opérations frauduleuses) qu'en valeur (montant des opérations ou des opérations frauduleuses). Le prestataire de services de paiement devrait indiquer les volumes et les valeurs en unités réelles, avec deux décimales pour les valeurs.
- 2.3 Un prestataire de services de paiement agréé ou une succursale établie dans un État membre de la zone euro devrait déclarer les valeurs en euros, tandis qu'un prestataire de services de paiement agréé ou une succursale établie dans un État membre ne participant pas à la zone euro devrait déclarer les valeurs dans la monnaie de cet État membre. Les prestataires de services de paiement déclarants devraient convertir les données relatives à la valeur des opérations ou des opérations frauduleuses libellées dans une monnaie autre que l'euro ou la monnaie officielle de l'État membre concerné dans la devise dans laquelle ils doivent déclarer, en utilisant les taux de change applicables à ces opérations ou le taux de change moyen de référence de la BCE pour la période de déclaration applicable.
- 2.4 Le prestataire de services de paiement ne devrait déclarer que les opérations de paiement qui ont été exécutées, y compris celles qui ont été initiées par un prestataire de services d'initiation de paiements. Les opérations frauduleuses bloquées avant leur exécution en raison d'une suspicion de fraude ne devraient pas être prises en compte.
- 2.5 Le prestataire de services de paiement devrait déclarer les informations statistiques selon une ventilation conforme à celle spécifiée dans l'orientation 7 et compilée à l'annexe 2.
- 2.6 Le prestataire de services de paiement devrait identifier la ventilation applicable en fonction du ou des service(s) de paiement et de l'instrument ou des instruments de paiement fourni(s), et soumettre les données correspondantes à l'autorité compétente.
- 2.7 Le prestataire de services de paiement devrait veiller à ce que toutes les données communiquées à l'autorité compétente puissent être vérifiées par recoupement, conformément à l'annexe 2.

- 2.8 Le prestataire de services de paiement devrait affecter chaque opération à une seule sous-catégorie pour chaque ligne de ventilation des données.
- 2.9 Dans le cas d'une série d'opérations de paiement en cours d'exécution, ou d'opérations de paiement frauduleuses en cours d'exécution, le prestataire de services de paiement devrait considérer chaque opération de paiement ou opération de paiement frauduleuse de la série comme une seule opération.
- 2.10 Le prestataire de services de paiement peut déclarer zéro («0») lorsqu'aucune opération ou opération frauduleuse n'est constatée pour la période de déclaration établie pour un indicateur donné. Lorsque le prestataire de services de paiement ne peut pas déclarer les données pour une ventilation spécifique parce que cette ventilation spécifique n'est pas applicable au prestataire de services de paiement, les données devraient être déclarées comme «NA» (non disponibles).
- 2.11 Afin d'éviter les doubles comptabilisations, le prestataire de services de paiement du payeur devrait soumettre les données en sa qualité d'émetteur (ou d'initiateur). Par exception, les données relatives aux paiements par carte devraient être déclarées à la fois par le prestataire de services de paiement du payeur et par le prestataire de services de paiement acquéreur du bénéficiaire. Les deux perspectives devraient être présentées séparément, avec des ventilations différentes comme détaillé à l'annexe 2. Lorsqu'une opération fait intervenir plusieurs prestataires de services de paiement acquéreurs, il appartient au prestataire lié contractuellement au bénéficiaire d'effectuer la déclaration. En outre, pour les prélèvements, les transactions devraient être déclarées uniquement par le prestataire de services de paiement du bénéficiaire, ces opérations étant initiées par le bénéficiaire.
- 2.12 Afin d'éviter les doubles comptabilisations lors du calcul de l'ensemble des opérations et des opérations frauduleuses pour tous les instruments de paiement, le prestataire de services de paiement effectuant les virements initiés par un prestataire de services d'initiation de paiements devrait indiquer la ventilation pour le volume et la valeur de l'ensemble des opérations et de l'ensemble des opérations frauduleuses initiées par l'intermédiaire d'un prestataire de services d'initiation de paiements, dans la ventilation A.

Orientation n° 3 Fréquence, délais et période de déclaration

- 3.1. Le prestataire de services de paiement devrait communiquer les données tous les six mois selon la ventilation indiquée en annexe 2.
- 3.2. Le prestataire de services de paiement bénéficiant d'une dérogation au titre de l'article 32 de la DSP2, ainsi que les établissements de monnaie électronique bénéficiant de la dérogation prévue par l'article 9 de la directive 2009/110/CE concernant l'accès à l'activité des établissements de monnaie électronique et son exercice ainsi que la surveillance prudentielle de ces établissements, devraient déclarer l'ensemble des données demandées en utilisant les formulaires proposés à l'annexe 2 sur une base annuelle seulement, en répartissant les données sur deux périodes de six mois.

- 3.3. Le prestataire de services de paiement devrait présenter les données le concernant dans les délais fixés par les autorités compétentes respectives.

Orientation n° 4 Répartition géographique

- 4.1 Le prestataire de services de paiement devrait procéder aux déclarations pour les opérations de paiement nationales, transfrontalières dans l'Espace économique européen (EEE) et transfrontalières hors EEE.
- 4.2 Pour les opérations de paiement sans carte et les opérations de paiement à distance par carte, les «opérations de paiement nationales» désignent les opérations de paiement initiées par un payeur ou par ou via un bénéficiaire, lorsque le prestataire de services de paiement du payeur et celui du bénéficiaire sont situés dans le même État membre.
- 4.3 Pour les opérations par carte de proximité, les «opérations de paiement nationales» désignent les opérations de paiement dans le cadre desquelles le prestataire de services de paiement du payeur (émetteur), le prestataire de services de paiement du bénéficiaire (acquéreur) et le point de vente (PdV) ou le distributeur automatique de billets (DAB) sont situés dans le même État membre.
- 4.4 Pour les succursales localisées dans l'EEE, les opérations de paiement nationales désignent les opérations de paiement dans le cadre desquelles le prestataire de services de paiement du payeur et celui du bénéficiaire sont tous deux situés l'État membre dans lequel la succursale est établie.
- 4.5 Pour les opérations de paiement sans carte et les opérations de paiement à distance par carte, le terme «opération de paiement transfrontalière dans l'EEE» désigne une opération de paiement initiée par un payeur ou par ou via un bénéficiaire, lorsque les prestataires de services de paiement respectifs du payeur et du bénéficiaire sont situés dans des États membres différents.
- 4.6 Pour les opérations par carte de proximité, les «opérations de paiement transfrontalières dans l'EEE» désignent les opérations de paiement dans le cadre desquelles le prestataire de services de paiement du payeur (émetteur) et celui du bénéficiaire (acquéreur) se trouvent dans des États membres différents ou dans le cadre desquelles le prestataire de services de paiement du payeur (émetteur) est situé dans un État membre différent de celui du PdV ou du DAB.
- 4.7 «Les opérations de paiement transfrontalières hors EEE» désignent les opérations de paiement initiées par un payeur ou par ou via un bénéficiaire dans le cadre desquelles le prestataire de services de paiement du payeur ou du bénéficiaire est situé en dehors de l'EEE tandis que l'autre prestataire est situé dans l'EEE.
- 4.8 Un prestataire de services de paiement offrant des services d'initiation de paiements devrait déclarer les opérations de paiement exécutées qu'il a initiées et les opérations de paiement frauduleuses exécutées qu'il a initiées conformément aux dispositions suivantes:
- a. Les «opérations de paiement nationales» désignent les opérations de paiement dans le cadre desquelles le prestataire de services d'initiation de paiements et le

prestataire de services de paiement gestionnaire de compte sont situés dans le même État membre;

b. Les «opérations de paiement transfrontalières au sein de l'EEE» désignent les opérations de paiement dans le cadre desquelles le prestataire de services d'initiation de paiements et le prestataire de services de paiement gestionnaire de compte sont situés dans des États membres différents;

c. Les «opérations de paiement transfrontalières hors EEE» désignent les opérations de paiement dans le cadre desquelles le prestataire de services d'initiation de paiements est situé dans l'EEE et le prestataire de services de paiement gestionnaire de compte est situé établi en dehors de l'EEE.

Orientation n° 5 Déclarations à l'autorité compétente

- 5.1. Le prestataire de services de paiement transmet sa déclaration à l'autorité compétente de l'État membre d'origine.
- 5.2. Le prestataire de services de paiement devrait enregistrer les données de tous ses agents fournissant des services de paiement dans l'EEE et agréger ces données avec les autres données le concernant, avant de les transmettre à l'autorité compétente d'origine. Dans ce cadre, le pays d'établissement de l'agent n'est pas pertinent pour déterminer la perspective géographique.
- 5.3. Dans le cadre des vérifications du suivi et des rapports prévus par l'article 29, paragraphe 2, de la DSP2, et par l'article 40 de la 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, la succursale d'un prestataire de services de paiement de l'EEE devrait soumettre ses déclarations à l'autorité compétente de l'État membre d'accueil où est établie la succursale, séparément des déclarations effectuées par le prestataire de services de paiement dans l'État membre d'origine.
- 5.4. Lors de la communication des données à l'autorité compétente, le prestataire de services de paiement devrait mentionner les informations d'identification mentionnées à l'annexe 1.

Orientation n° 6 Enregistrement/dates de référence

- 6.1 La date d'enregistrement que les prestataires de services de paiement doivent prendre en compte pour les opérations de paiement et les opérations de paiement frauduleuses aux fins de la déclaration statistique est le jour où la transaction a été exécutée conformément à la DSP2. Dans le cas d'une série d'opérations, la date enregistrée devrait être la date à laquelle chaque opération de paiement a été exécutée.
- 6.2 Le prestataire de services de paiement devrait déclarer toutes les opérations de paiement frauduleuses à partir du moment où la fraude a été détectée, par exemple à la suite d'une

réclamation d'un client ou par d'autres moyens, indépendamment de la question de savoir si le dossier lié au paiement frauduleux a été clôturé au moment de la déclaration.

- 6.3 Le prestataire de services de paiement devrait déclarer tous les ajustements apportés aux données, à tout le moins lorsqu'elles concernent une période de déclaration antérieure d'au moins un an, au cours de la période déclarative suivant la découverte des informations nécessitant les ajustements. Le prestataire de services de paiement devrait indiquer que les données communiquées sont des chiffres révisés applicables à la période écoulée et indiquer cette révision conformément à la méthodologie établie par l'autorité compétente concernée.

Orientation n° 7 Ventilation des données

- 7.1 Pour les opérations de paiement en monnaie électronique telles que définies dans la directive 2009/110/CE, le prestataire de services de paiement devrait fournir les données conformément à la ventilation des données F de l'annexe 2.
- 7.2 Lorsqu'il fournit des données sur les opérations en monnaie électronique, le prestataire de services de paiement devrait inclure les opérations de paiement en monnaie électronique
- a. pour lesquelles le PSP du payeur est identique au PSP du bénéficiaire, ou
 - b. pour lesquelles l'opération a été réalisée avec une carte dotée d'une fonctionnalité de monnaie électronique.
- 7.3 Le prestataire de services de paiement devrait, aux fins des opérations de paiement en monnaie électronique, fournir les données sur les volumes et les valeurs de l'ensemble des opérations de paiement, ainsi que sur les volumes et les valeurs des opérations de paiement frauduleuses, ventilées comme suit:
- a. la répartition géographique,
 - b. le canal de paiement,
 - c. la méthode d'authentification,
 - d. le motif de dérogation à l'application d'une authentification forte du client [par référence aux dérogations exposées au chapitre III des Normes techniques de réglementation en matière d'authentification forte du client et de normes communes et sécurisées de communication du règlement délégué [UE] 2018/389 de la Commission, ► A1, ou à l'une des catégories «Opérations initiées par des commerçants» et «Autres», le cas échéant], et
 - e. les types de fraude.
- 7.4 Pour les services de transmission de fonds, le prestataire de services de paiement devrait fournir les données conformément à la ventilation des données G de l'annexe 2 et comme spécifié dans l'orientation 1.3. Le prestataire de services de paiement qui propose ce type de service devrait communiquer des données sur les volumes et les valeurs de l'ensemble des

opérations de paiement et de toutes les opérations de paiement frauduleuses indiquées dans l'orientation 2.1, avec la perspective géographique.

- 7.5 Lorsqu'il fournit des services d'initiation de paiement, le prestataire de services de paiement devrait communiquer les données conformément à la ventilation des données H de l'annexe 2. Le prestataire de services de paiement devrait déclarer les opérations de paiement exécutées qu'il a initiées et les opérations de paiement frauduleuses exécutées qu'il a initiées, tant en volume qu'en valeur.
- 7.6 Pour les opérations de paiement soumises à la ventilation des données H de l'annexe 2, le prestataire de services de paiement qui propose des services d'initiation de paiements devrait enregistrer et communiquer des données sur les volumes et les valeurs selon les ventilations suivantes:
- a. la répartition géographique,
 - b. l'instrument de paiement,
 - c. le canal de paiement, et
 - d. la méthode d'authentification.
- 7.7 Un prestataire de services de paiement qui ne gère pas le compte de l'utilisateur du service de paiement mais émet et exécute des paiements par carte (un émetteur d'instruments de paiement par carte) devrait fournir les données sur les volumes et les valeurs conformément à la ventilation des données C et/ou E de l'annexe 2. Lorsque de telles données sont fournies, le prestataire de services de paiement gestionnaire de compte devrait s'assurer que les opérations ne font pas l'objet de doubles déclarations.
- 7.8 Le prestataire de services de paiement offrant des services de virement et de paiement par carte devrait fournir les données conformément aux ventilations A, C et/ou D de l'annexe 2, en fonction de l'instrument de paiement utilisé pour une opération de paiement donnée et du rôle du prestataire des services de paiement. Les données à transmettre comprennent:
- a. la répartition géographique,
 - b. le canal de paiement,
 - c. la méthode d'authentification,
 - d. le motif de dérogation à l'application d'une authentification forte du client [par référence aux dérogations à l'authentification forte du client établies au chapitre III des NTR en matière d'authentification forte du client et de normes communes et sécurisées de communication, ► A1, ou à l'une des catégories «Opérations initiées par des commerçants» et «Autres», le cas échéant],
 - e. les types de fraude,
 - f. la fonction de la carte pour la ventilation des données C et D, et

- g. les opérations de paiement initiées via un prestataire de services d'initiation de paiements pour la ventilation des données A.
- 7.9 Le prestataire de services de paiement devrait fournir les données conformément à la ventilation des données A de l'annexe 2 pour l'ensemble des opérations de paiement et des opérations de paiement frauduleuses exécutées au moyen de virements.
- 7.10 Le prestataire de services de paiement devrait fournir les données conformément à la ventilation des données B de l'annexe 2 pour l'ensemble des opérations de paiement et des opérations de paiement frauduleuses exécutées au moyen de prélèvements. Les données à transmettre comprennent:
 - a. la répartition géographique,
 - b. le canal utilisé pour donner le consentement, et
 - c. les types de fraude.
- 7.11 Le prestataire de services de paiement émetteur devrait fournir les données conformément à la ventilation des données C de l'annexe 2 pour l'ensemble des opérations de paiement et des opérations de paiement frauduleuses réalisées au moyen d'une carte de paiement, lorsque le prestataire de services de paiement est également le prestataire de services de paiement du payeur.
- 7.12 Le prestataire de services de paiement acquéreur devrait fournir les données conformément à la ventilation des données D de l'annexe 2 pour toutes les opérations de paiement et toutes les opérations de paiement frauduleuses réalisées au moyen d'une carte de paiement, lorsque le prestataire de services de paiement est également le prestataire de services de paiement du bénéficiaire.
- 7.13 Le prestataire de services de paiement qui fournit des données conformément aux ventilations de données A à F de l'annexe 2 devrait déclarer l'ensemble des pertes résultant d'une fraude, par porteur de responsabilité, au cours de la période considérée.
- 7.14 Le prestataire de services de paiement qui déclare des opérations de paiement par carte conformément aux ventilations C et D de l'annexe 2 devrait exclure les retraits d'espèces et les dépôts en espèces.
- 7.15 Le prestataire de services de paiement (émetteur) devrait fournir les données conformément à la ventilation des données E de l'annexe 2 pour tous les retraits d'espèces et tous les retraits d'espèces frauduleux effectués au moyen d'une carte à partir ► **A1** de guichets automatiques (y compris au moyen d'applications), de guichets bancaires et auprès de commerçants («cashback»).

3.2. Orientations relatives à la déclaration des données agrégées en matière de fraude par les autorités compétentes à l'ABE et à la BCE

Orientation n° 1 Opérations de paiement et opérations de paiement frauduleuses

- 1.1. Aux fins de la déclaration des données statistiques en matière de fraude à l'ABE et à la BCE conformément aux présentes orientations et à l'article 96, paragraphe 6, de la DSP2, l'autorité compétente devrait déclarer pour chaque période de référence:
 - a. toute opération de paiement non autorisée effectuée, y compris à la suite de la perte, du vol ou de l'appropriation illicite de données de paiement sensibles ou d'un instrument de paiement, qu'elle soit détectable ou non par le payeur avant un paiement et résultant ou non d'une négligence grave du payeur ou exécutée en l'absence de consentement du payeur («opération de paiement non autorisée»); et
 - b. toute opération de paiement effectuée à la suite d'une manipulation du payeur par le fraudeur, ayant pour effet d'émettre un ordre de paiement ou de donner instruction de le faire au prestataire de services de paiement, de bonne foi, à un compte de paiement qu'il estime appartenir à un bénéficiaire légitime («manipulation du payeur»).
- 1.2. Aux fins de l'orientation 1.1, l'autorité compétente ne devrait déclarer que les opérations de paiement initiées et exécutées (acquises, le cas échéant) par les prestataires de services de paiement (y compris les émetteurs de cartes de paiement, le cas échéant). L'autorité compétente ne devrait pas déclarer les données sur les opérations de paiement qui, quel que soit leur lien avec l'une des situations visées dans l'orientation 1.1, n'ont pas été exécutées et n'ont pas entraîné de transfert de fonds conformément aux dispositions de la DSP2.
- 1.3. Les autorités compétentes devraient déclarer l'ensemble des opérations de paiement et des opérations de paiement frauduleuses conformément aux dispositions suivantes:
 - a. s'agissant des opérations de paiement sans carte et des opérations de paiement par carte à distance, les «opérations de paiement nationales» désignent les opérations de paiement initiées par un payeur ou par ou via un bénéficiaire, dans le cadre desquelles le prestataire de services de paiement du payeur et celui du bénéficiaire sont situés dans le même État membre,

- b. Pour les succursales établies dans l'EEE, les opérations de paiement nationales désignent les opérations de paiement dans le cadre desquelles le prestataire de services de paiement du payeur et celui du bénéficiaire sont tous deux situés dans l'État membre dans lequel la succursale est établie.
- c. S'agissant des opérations de paiement sans carte et des opérations de paiement par carte à distance, les «opérations de paiement transfrontalières dans l'EEE» désignent les opérations de paiement initiées par un payeur ou par ou via un bénéficiaire, dans le cadre desquelles le prestataire de services de paiement du payeur et celui du bénéficiaire sont situés dans des États membres différents.
- d. S'agissant des opérations de paiement par carte en proximité, les «opérations de paiement nationales» désignent les opérations de paiement dans le cadre desquelles le prestataire de services de paiement (émetteur) du payeur et celui du bénéficiaire (acquéreur), ainsi que le PdV ou le DAB utilisé, sont situés dans le même État membre. Si le prestataire de services de paiement du payeur et le prestataire de services de paiement du bénéficiaire sont situés dans des États membres différents ou si le prestataire de services de paiement du payeur (émetteur) est situé dans un État membre différent de celui où se trouve le PdV ou le DAB, l'opération est une «opération de paiement transfrontalière dans l'EEE».
- e. «Les opérations de paiement transfrontalières en hors EEE» désignent les opérations de paiement initiées par un payeur ou par ou via un bénéficiaire dans le cadre desquelles le prestataire de services de paiement du payeur ou du bénéficiaire est situé en dehors de l'EEE et l'autre prestataire est situé dans l'EEE.
- f. Le «total des opérations de paiement frauduleuses» désigne l'ensemble des opérations visées dans l'orientation 1.1, que le montant de l'opération de paiement frauduleuse ait ou non été recouvré.
- g. La «modification d'un ordre de paiement par le fraudeur» est une opération non autorisée telle que définie dans l'orientation 1.1, point a), et désigne une situation dans laquelle le fraudeur intercepte et modifie un ordre de paiement légitime à un moment donné de la communication électronique entre le dispositif du payeur et le prestataire de services de paiement (par exemple au moyen de logiciels malveillants ou d'attaques de type «man in the middle») ou modifie l'instruction de paiement dans le système du prestataire de services de paiement avant que l'ordre de paiement ne soit compensé et réglé.
- h. L'«émission d'un ordre de paiement par le fraudeur» est une opération non autorisée telle que définie dans l'orientation 1.1, point a), et désigne une situation dans laquelle un ordre de paiement factice est émis par un fraudeur qui a préalablement obtenu les données de paiement sensibles ou à caractère personnel du payeur/du bénéficiaire par des moyens frauduleux.

- 1.4. Les autorités compétentes devraient communiquer les données fournies par les prestataires de services de paiement qui proposent des services d'initiation de paiements selon les modalités suivantes:
- a. les «opérations de paiement nationales» désignent les opérations de paiement dans le cadre desquelles le prestataire de services d'initiation de paiements et le prestataire de services de paiement gestionnaire de compte sont situés dans le même État membre.
 - b. Les «opérations de paiement transfrontalières au sein de l'EEE» désignent les opérations de paiement dans le cadre desquelles le prestataire de services d'initiation de paiements et le prestataire de services de paiement gestionnaire de compte sont situés dans des États membres différents.
 - c. Les «opérations de paiement transfrontalières hors EEE» désignent les opérations de paiement dans le cadre desquelles le prestataire de services de paiement est situé dans l'EEE et le prestataire de services de paiement gestionnaire de compte est situé en dehors de l'EEE.

Orientation n° 2 Collecte et agrégation des données

- 2.1 L'autorité compétente devrait communiquer des informations statistiques sur:
- a. l'ensemble des opérations de paiement, conformément aux différentes ventilations définies à l'annexe 2 et dans l'orientation 1,2; et
 - b. l'ensemble des opérations de paiement frauduleuses, conformément aux différentes ventilations définies à l'annexe 2 et dans l'orientation 1.3, point f).
- 2.2 L'autorité compétente devrait déclarer les informations statistiques listées dans l'orientation 2.1, tant en volume (c'est-à-dire le nombre d'opérations ou d'opérations frauduleuses) qu'en valeur (c'est-à-dire le montant des opérations ou des opérations frauduleuses). L'autorité compétente devrait indiquer les volumes et les valeurs en unités réelles, avec deux décimales pour les valeurs.
- 2.3 L'autorité compétente devrait déclarer les valeurs en euros. L'autorité compétente devrait convertir les données relatives aux opérations (frauduleuses ou non) libellées dans une monnaie autre que l'euro, en utilisant les taux de change applicables à ces opérations ou le taux de change de référence moyen de la BCE pour la période de référence applicable.
- 2.4 L'autorité compétente peut déclarer zéro («0») lorsqu'aucune opération ou opération frauduleuse n'est constatée pendant la période de déclaration établie pour un indicateur donné.
- 2.5 L'autorité compétente devrait agréger les données collectées dans son État membre auprès des destinataires des présentes orientations, en additionnant les chiffres communiqués pour chaque prestataire de services de paiement individuel, conformément aux ventilations de l'annexe 2.

- 2.6 L'autorité compétente devrait définir les procédures de communication sécurisées et le format de communication des données par les prestataires de services de paiement. L'autorité compétente devrait également veiller à ce que les prestataires de services de paiement disposent d'un délai approprié pour garantir la qualité des données et pour tenir compte du retard potentiel dans la déclaration des opérations de paiement frauduleuses.
- 2.7 L'autorité compétente devrait veiller à ce que les données communiquées au titre des présentes orientations puissent être vérifiées par recoupement et être utilisées par l'ABE et la BCE conformément aux ventilations de l'annexe 2.

Orientation n° 3 La déclaration des données en pratique

- 3.1 L'autorité compétente devrait déclarer les volumes et les valeurs des opérations de paiement et des opérations de paiement frauduleuses conformément aux orientations 2.1 et 2.2. Pour éviter les doubles comptabilisations, les données ne devraient pas être agrégées entre les différentes ventilations de l'annexe 2.
- 3.2 L'autorité compétente devrait déclarer les ajustements apportés aux données concernant toute opération de paiement ou toute opération de paiement frauduleuse, déclarée au cours de toute période de déclaration passée, dès la période de déclaration suivante, après avoir obtenu les informations nécessitant les ajustements auprès d'un prestataire de services de paiement donné et jusqu'à 13 mois après l'exécution (et/ou l'acquisition) de l'opération, afin de permettre à l'utilisateur du service de paiement d'exercer son droit d'aviser le prestataire de services de paiement au plus tard 13 mois après l'exécution de l'opération, conformément à l'article 71 de la DSP2.
- 3.3 Les autorités compétentes devraient à tout moment préserver la confidentialité et l'intégrité des informations stockées et échangées avec l'ABE et la BCE et s'identifier de manière appropriée auprès de l'ABE et de la BCE.
- 3.4 L'autorité compétente devrait envoyer les données agrégées à la BCE et à l'ABE dans un délai de six mois à compter du jour suivant la fin de la période de déclaration.
- 3.5 L'autorité compétente devrait convenir avec la BCE et l'ABE des procédures de communication sécurisées et du format spécifique dans lequel l'autorité compétente devrait communiquer les données.

Orientation n° 4 Coopération entre autorités compétentes

- 4.1 Lorsque plusieurs autorités compétentes sont établies dans un État membre au titre de la DSP2, les autorités compétentes devraient coordonner la collecte des données afin de garantir qu'un seul ensemble de données est communiqué pour cet État membre à la BCE et à l'ABE.

- 4.2 À la demande de l'autorité compétente d'un État membre d'origine, l'autorité compétente d'un État membre d'accueil devrait mettre à disposition les informations et les données que les succursales établies lui ont communiquées.

Annexe 1 - Données générales à fournir par tous les prestataires de services de paiement déclarants

Données d'identification générales sur le prestataire de services de paiement déclarant

Nom: nom complet du prestataire de services de paiement soumis à la procédure de déclaration des données tel qu'il figure dans le registre national applicable pour les établissements de crédit, les établissements de paiement ou les établissements de monnaie électronique.

Numéro d'identification unique: numéro d'identification unique pertinent utilisé dans chaque État membre pour identifier le prestataire de services de paiement, le cas échéant.

Numéro d'agrément: numéro d'agrément de l'État membre d'origine, le cas échéant.

Pays d'agrément: État membre d'origine dans lequel l'agrément a été octroyé.

Contact principal: le nom et le prénom de la personne chargée de déclarer les données ou, si un tiers déclare les données pour le compte du prestataire de services de paiement, le nom et le prénom de la personne responsable du service de gestion des données ou d'un service similaire, au niveau du prestataire de services de paiement.

Adresse électronique: l'adresse électronique à laquelle toute demande de précisions devrait être envoyée, si nécessaire. Il peut s'agir d'une adresse électronique personnelle ou professionnelle.

Numéro de téléphone: le numéro de téléphone auquel toute demande de précisions peut être formulée, si nécessaire. Il peut s'agir d'un numéro de téléphone personnel ou professionnel.

Ventilation des données

Toutes les données déclarées par les PSP sur la base des différentes ventilations exposées à l'annexe 2 devraient correspondre à la répartition géographique définie ci-dessous et indiquer à la fois le nombre d'opérations (*unités réelles, total pour la période*) et la valeur des opérations (*EUR/unités réelles de la devise locale, total pour la période*).

	Valeur et volume
Domaine	National; Transfrontalier <i>au sein de l'EEE</i> ; et Transfrontalier <i>hors EEE</i>

Annexe 2 – Modèles de déclaration à l'intention des prestataires de services de paiement

A- Ventilation des données pour les virements

	Libellé	Opérations de paiement	Opérations de paiement frauduleuses
1	Virements	X	X
1.1	Dont initiation par des prestataires de services d'initiation de paiement	X	X
1.2	Dont opérations initiées de manière non électronique	X	X
1.3	Dont initiation électronique	X	X
1.3.1	Dont opérations initiées via un canal de paiement à distance	X	X
1.3.1.1	Dont opération avec authentification client forte	X	X
	<i>dont virements frauduleux par type de fraude:</i>		
1.3.1.1.1	Émission d'un ordre de paiement par le fraudeur		X
1.3.1.1.2	Modification d'un ordre de paiement par le fraudeur		X
1.3.1.1.3	Manipulation du payeur par le fraudeur ayant pour effet d'émettre un ordre de paiement		X
1.3.1.2	Dont opération avec authentification client non forte	X	X
	<i>dont virements frauduleux par type de fraude:</i>		
1.3.1.2.1	Émission d'un ordre de paiement par le fraudeur		X
1.3.1.2.2	Modification d'un ordre de paiement par le fraudeur		X
1.3.1.2.3	Manipulation du payeur par le fraudeur ayant pour effet d'émettre un ordre de paiement		X
	<i>dont ventilation par motif d'omission d'authentification client forte</i>		

1.3.1.2.4	Faible montant (article16 NTR)	X	X
1.3.1.2.5	Paiement à soi-même (article15 NTR)	X	X
1.3.1.2.6	Bénéficiaire de confiance (article13 NTR)	X	X
1.3.1.2.7	Opération récurrente (article14 NTR)	X	X
1.3.1.2.8	Utilisation de procédures et protocoles de paiement d'entreprise sécurisés (article 17 NTR)	X	X
1.3.1.2.9	Analyse des risques liés à l'opération (article18 NTR)	X	X
1.3.2	Dont initiation via un canal de paiement non distant	X	X
1.3.2.1	Dont opérations avec authentification client forte	X	X
	<i>dont virements frauduleux par type de fraude</i>		
1.3.2.1.1	Émission d'un ordre de paiement par le fraudeur		X
1.3.2.1.2	Modification d'un ordre de paiement par le fraudeur		X
1.3.2.1.3	Manipulation du payeur par le fraudeur ayant pour effet d'émettre un ordre de paiement		X
1.3.2.2	Dont opérations avec authentification client non forte	X	X
	<i>dont virements frauduleux par type de fraude:</i>		
1.3.2.2.1	Émission d'un ordre de paiement par le fraudeur		X
1.3.2.2.2	Modification d'un ordre de paiement par le fraudeur		X
1.3.2.2.3	Manipulation du payeur par le fraudeur ayant pour effet d'émettre un ordre de paiement		X
	<i>dont ventilation par motif d'omission d'authentification client forte</i>		
1.3.2.2.4	Paiement à soi-même (article15 NTR)	X	X
1.3.2.2.5	Bénéficiaire de confiance (article13 NTR)	X	X
1.3.2.2.6	Opération récurrente (article14 NTR)	X	X
1.3.2.2.7	Paiement sans contact de faible montant (article 11 NTR)	X	X
1.3.2.2.8	Automates de paiement des frais de transport et de parking (article 12 NTR)	X	X

Pertes dues à une fraude, par porteur de responsabilité:	Pertes totales
Le prestataire de services de paiement déclarant	X

L'utilisateur du service de paiement (payeur)	X
Autres	X

Validation

1.2 + 1.3 = 1; 1.1 n'est pas égal à 1 mais est un sous-ensemble de 1
1.3.1 + 1.3.2 = 1.3
1.3.1.1 + 1.3.1.2 = 1.3.1
1.3.2.1 + 1.3.2.2 = 1.3.2
1.3.1.1.1 + 1.3.1.1.2 + 1.3.1.1.3 = montant des opérations de paiement frauduleuses de 1.3.1.1; 1.3.1.2.1 + 1.3.1.2.2 + 1.3.1.2.3 = chiffre de opérations de paiement frauduleuses de 1.3.1.2; 1.3.2.1.1 + 1.3.2.1.2 + 1.3.2.1.3 = chiffre des opérations de paiement frauduleuses de 1.3.2.1; 1.3.2.2.1 + 1.3.2.2.2 + 1.3.2.2.3 = montant des opérations de paiement frauduleuses de 1.3.2.2
1.3.1.2.4 + 1.3.1.2.5 + 1.3.1.2.6 + 1.3.1.2.7 + 1.3.1.2.8 + 1.3.1.2.9 = 1.3.1.2
1.3.2.2.4 + 1.3.2.2.5 + 1.3.2.2.6 + 1.3.2.2.7 + 1.3.2.2.8 = 1.3.2.2

B- Ventilation des données pour les prélèvements

	Libellé	Opérations de paiement	Opérations de paiement frauduleuses
2	Prélèvements	X	X
2.1	Dont ceux pour lesquels consentement donné via un mandat électronique	X	X
	<i>dont prélèvements frauduleux par type de fraude:</i>		
2.1.1.1	Opérations de paiement non autorisées		X
2.1.1.2	Manipulation du payeur par le fraudeur ayant pour effet d'obtenir un prélèvement		X
2.2	Dont ceux pour lesquels consentement donné sous une autre forme qu'un mandat électronique	X	X
	<i>dont prélèvements frauduleux par type de fraude:</i>		
2.2.1.1	Opérations de paiement non autorisées		X
2.2.1.2	Manipulation du payeur par le fraudeur ayant pour effet d'obtenir un prélèvement		X

Pertes dues à une fraude, par porteur de responsabilité:	Pertes totales
Le prestataire de services de paiement déclarant	X
L'utilisateur du service de paiement (bénéficiaire)	X
Autres	X

Validation

2.1 + 2.2 = 2
2.1.1.1 + 2.1.1.2 = montant des opérations de paiement frauduleuses de 2.1
2.2.1.1 + 2.2.1.2 = montant des opérations de paiement frauduleuses de 2.2

C- Ventilation des données pour les opérations de paiement par carte devant être déclarées par le prestataire de services de paiement ► A1 émetteur

	Libellé	Opérations de paiement	Opérations de paiement frauduleuses
3	Paiements par carte (excepté les cartes dotées uniquement d'une fonction de monnaie électronique)	X	X
3.1	Dont opérations initiées de manière non électronique	X	X
3.2	Dont opérations initiées par voie électronique	X	X
3.2.1	Dont opérations initiées via un canal de paiement à distance	X	X
	<i>dont ventilation par fonction de la carte:</i>		
3.2.1.1.1	Paiements par carte dotée d'une fonction de prélèvement	X	X
3.2.1.1.2	Paiements par carte dotée d'une fonction de crédit ou de débit différé	X	X
3.2.1.2	Dont opérations avec authentification client forte	X	X
	<i>dont paiements frauduleux par carte, par type de fraude:</i>		
3.2.1.2.1	Émission d'un ordre de paiement par le fraudeur		X
3.2.1.2.1.1	Carte perdue ou volée		X
3.2.1.2.1.2	Carte non reçue		X
3.2.1.2.1.3	Carte contrefaite		X
3.2.1.2.1.4	Vol des informations contenues dans la carte		X
3.2.1.2.1.5	Autres		X
3.2.1.2.2	Modification d'un ordre de paiement par le fraudeur		X
3.2.1.2.3	Manipulation du payeur ayant pour effet d'obtenir un paiement par carte		X
3.2.1.3	Dont authentification via une authentification client non forte	X	X
	<i>dont paiements frauduleux par carte, par type de fraude:</i>		
3.2.1.3.1	Émission d'un ordre de paiement par le fraudeur		X
3.2.1.3.1.1	Carte perdue ou volée		X
3.2.1.3.1.2	Carte non reçue		X
3.2.1.3.1.3	Carte contrefaite		X
3.2.1.3.1.4	Vol des informations contenues dans la carte		X
3.2.1.3.1.5	Autres		X

3.2.1.3.2	Modification d'un ordre de paiement par le fraudeur		X
3.2.1.3.3	Manipulation du payeur ayant pour effet d'obtenir un paiement par carte		X
	<i>dont ventilation par motif d'omission d'authentification client forte</i>		
3.2.1.3.4	Faible montant (article 16 NTR)	X	X
3.2.1.3.5	Bénéficiaire de confiance (article 13 NTR)	X	X
3.2.1.3.6	Opération récurrente (article 14 NTR)	X	X
3.2.1.3.7	Utilisation de procédures et protocoles de paiement d'entreprise sécurisés (article 17 NTR)	X	X
3.2.1.3.8	Analyse des risques liés à l'opération (article 18 NTR)	X	X
► A1 3.2.1.3.9	Opérations initiées par des commerçants ²	X	X
► A1 3.2.1.3.10	Autres	X	X
3.2.2	Dont initiation via un canal de paiement non distant	X	X
	<i>dont ventilation par fonction de la carte:</i>		
3.2.2.1.1	Paiements par carte dotée d'une fonction de débit	X	X
3.2.2.1.2	Paiements par carte dotée d'une fonction de crédit ou de débit différé	X	X
3.2.2.2	Dont opérations avec authentification client forte	X	X
	<i>dont paiements frauduleux par carte, par type de fraude:</i>		
3.2.2.2.1	Émission d'un ordre de paiement par le fraudeur		X
3.2.2.2.1.1	Carte perdue ou volée		X
3.2.2.2.1.2	Carte non reçue		X
3.2.2.2.1.3	Carte contrefaite		X
3.2.2.2.1.4	Autres		X
3.2.2.2.2	Modification d'un ordre de paiement par le fraudeur		X
3.2.2.2.3	Manipulation du payeur ayant pour effet d'obtenir un paiement par carte		X
3.2.2.3	Dont opérations avec authentification client non forte	X	X
	<i>dont paiements frauduleux par carte, par type de fraude:</i>		
3.2.2.3.1	Émission d'un ordre de paiement par le fraudeur		X
3.2.2.3.1.1	Carte perdue ou volée		X

² ► A1 c'est-à-dire des opérations de paiement par carte qui respectent les exigences précisées par la Commission européenne dans les Q&A 2018_4131 et Q&A 2018_4031 et qui sont dès lors considérées comme initiées par le bénéficiaire et non soumises à l'exigence visée à l'article 97 de la DSP2 relative à l'application de l'authentification forte du client

3.2.2.3.1.2	Carte non reçue		X
3.2.2.3.1.3	Carte contrefaite		X
3.2.2.3.1.4	Autres		X
3.2.2.3.2	Modification d'un ordre de paiement par le fraudeur		X
3.2.2.3.3	Manipulation du payeur ayant pour effet d'obtenir un paiement par carte		X
	<i>dont ventilation par motif d'omission d'authentification client forte</i>		
3.2.2.3.4	Bénéficiaire de confiance (article13 NTR)	X	X
3.2.2.3.5	Opération récurrente (article14 NTR)	X	X
3.2.2.3.6	Paiement sans contact de faible montant (article16 NTR)	X	X
3.2.2.3.7	Automates de paiement des frais de transport et de parking (article 12 NTR)	X	X
► A1 3.2.2.3.8	Autres	X	X

Pertes dues à une fraude, par porteur de responsabilité :	Pertes totales
Le prestataire de services de paiement déclarant	X
L'utilisateur du service de paiement (payeur)	X
Autres	X

Validation

3.1 + 3.2 = 3
3.2.1 + 3.2.2 = 3.2
3.2.1.1.1 + 3.2.1.1.2 = 3.2.1; 3.2.2.1.1 + 3.2.2.1.2 = 3.2.2
3.2.1.2 + 3.2.1.3 = 3.2.1; 3.2.2.2 + 3.2.2.3 = 3.2.2
3.2.1.2.1 + 3.2.1.2.2 + 3.2.1.2.3 = montant des opérations de paiement frauduleuses de 3.2.1.2; 3.2.1.3.1 + 3.2.1.3.2 + 3.2.1.3.3 = chiffre d'opération de paiement frauduleuse de 3.2.1.3; 3.2.2.2.1 + 3.2.2.2.2 + 3.2.2.2.3 =montant des opérations de paiement frauduleuse de3.2.2.2; 3.2.2.3.1 + 3.2.2.3.2 + 3.2.2.3.3 =montant des opérations de paiement frauduleuses de 3.2.2.3
3.2.1.2.1.1 + 3.2.1.2.1.2 + 3.2.1.2.1.3 + 3.2.1.2.1.4 + 3.2.1.2.1.5 = montant des opérations de paiement frauduleuses de 3.2.1.2.1; 3.2.1.3.1.1 + 3.2.1.3.1.2 + 3.2.1.3.1.3 + 3.2.1.3.1.4 + 3.2.1.3.1.5 = montant des opérations de paiement frauduleuses de 3.2.1.3.1; 3.2.2.2.1.1 + 3.2.2.2.1.2 + 3.2.2.2.1.3 + 3.2.2.2.1.4 =montant des opérations de paiement frauduleuses de3.2.2.2.1; 3.2.2.3.1.1 + 3.2.2.3.1.2 + 3.2.2.3.1.3 + 3.2.2.3.1.4 =montant des opérations de paiement frauduleuses de 3.2.2.3.1

► **A1** 3.2.1.3.4 + 3.2.1.3.5 + 3.2.1.3.6 + 3.2.1.3.7 + 3.2.1.3.8 + 3.2.1.3.9 + 3.2.1.3.10 = 3.2.1.3; 3.2.2.3.4 + 3.2.2.3.5 + 3.2.2.3.6 + 3.2.2.3.7 + 3.2.2.3.8 = 3.2.2.3

D- Ventilation des données pour les opérations de paiement par carte devant être déclarées par le prestataire de services de paiement ► A1 acquéreur (lié contractuellement avec l'utilisateur du service de paiement)

	Libellé	Opérations de paiement	Opérations de paiement frauduleuses
4	Paiements par carte acquis (excepté les cartes dotées uniquement d'une fonction de monnaie électronique)	X	X
4.1	Dont opérations initiées de manière non électronique	X	X
4.2	Dont opérations initiées par voie électronique	X	X
4.2.1	Dont acquis via un canal à distance	X	X
	<i>dont ventilation par fonction de la carte:</i>		
4.2.1.1.1	Paiements par carte dotée d'une fonction de prélèvement	X	X
4.2.1.1.2	Paiements par carte dotée d'une fonction de crédit ou de débit différé	X	X
4.2.1.2	Dont opérations avec authentification client forte	X	X
	<i>dont paiements frauduleux par carte, par type de fraude:</i>		
4.2.1.2.1	Émission d'un ordre de paiement par le fraudeur		X
4.2.1.2.1.1	Carte perdue ou volée		X
4.2.1.2.1.2	Carte non reçue		X
4.2.1.2.1.3	Carte contrefaite		X
4.2.1.2.1.4	Vol des informations contenues dans la carte		X
4.2.1.2.1.5	Autres		X
4.2.1.2.2	Modification d'un ordre de paiement par le fraudeur		X
4.2.1.2.3	Manipulation du payeur ayant pour effet d'obtenir un paiement par carte		X
4.2.1.3	Dont opérations avec authentification client non forte	X	X
	<i>dont paiements frauduleux par carte, par type de fraude:</i>		
4.2.1.3.1	Émission d'un ordre de paiement par le fraudeur		X
4.2.1.3.1.1	Carte perdue ou volée		X
4.2.1.3.1.2	Carte non reçue		X
4.2.1.3.1.3	Carte contrefaite		X
4.2.1.3.1.4	Vol des informations contenues dans la carte		X

4.2.1.3.1.5	Autres		X
4.2.1.3.2	Modification d'un ordre de paiement par le fraudeur		X
4.2.1.3.3	Manipulation du payeur ayant pour effet d'obtenir un paiement par carte		X
	<i>dont ventilation par motif d'omission d'authentification client forte</i>		
4.2.1.3.4	Faible montant (article16 NTR)	X	X
4.2.1.3.5	Opération récurrente (article14 NTR)	X	X
4.2.1.3.6	Analyse des risques liés à l'opération (article18 NTR)	X	X
► A1 4.2.1.3.7	Opérations initiées par des commerçants ³	X	X
► A1 4.2.1.3.8	Autres	X	X
4.2.2	Dont acquis via un canal non distant	X	X
	<i>dont ventilation par fonction de la carte:</i>		
4.2.2.1.1	Paiements par carte dotée d'une fonction de prélèvement	X	X
4.2.2.1.2	Paiements par carte dotée d'une fonction de crédit ou de débit différé	X	X
4.2.2.2	Dont opérations avec authentification client forte	X	X
	<i>dont paiements frauduleux par carte, par type de fraude:</i>		
4.2.2.2.1	Émission d'un ordre de paiement par le fraudeur		X
4.2.2.2.1.1	Carte perdue ou volée		X
4.2.2.2.1.2	Carte non reçue		X
4.2.2.2.1.3	Carte contrefaite		X
4.2.2.2.1.4	Autres		X
4.2.2.2.2	Modification d'un ordre de paiement par le fraudeur		X
4.2.2.2.3	Manipulation du payeur ayant pour effet d'obtenir un paiement par carte		X
4.2.2.3	Dont opérations avec authentification client non forte	X	X
	<i>dont paiements frauduleux par carte, par type de fraude:</i>		
4.2.2.3.1	Émission d'un ordre de paiement par le fraudeur		X
4.2.2.3.1.1	Carte perdue ou volée		X
4.2.2.3.1.2	Carte non reçue		X
4.2.2.3.1.3	Carte contrefaite		X
4.2.2.3.1.4	Autres		X

³ ► A1 Voir la note de bas de page 4

4.2.2.3.2	Modification d'un ordre de paiement par le fraudeur		X
4.2.2.3.3	Manipulation du payeur ayant pour effet d'obtenir un paiement par carte <i>dont ventilation par motif d'omission d'authentification client forte</i>		X
4.2.2.3.4	Opération récurrente (article14 NTR)	X	X
4.2.2.3.5	Paiement sans contact de faible montant (article16 NTR)	X	X
4.2.2.3.6	Automates de paiement des frais de transport et de parking (article 12 NTR)	X	X
► A1 4.2.2.3.7	Autres	X	X

Pertes dues à une fraude, par porteur de responsabilité:	Pertes totales
Le prestataire de services de paiement déclarant	X
L'utilisateur du service de paiement (bénéficiaire)	X
Autres	X

Validation

4.1 + 4.2 = 4
4.2.1 + 4.2.2 = 4.2
4.2.1.1.1 + 4.2.1.1.2 = 4.2.1; 4.2.2.1.1 + 4.2.2.1.2 = 4.2.2
4.2.1.2 + 4.2.1.3 = 4.2.1; 4.2.2.2 + 4.2.2.3 = 4.2.2
4.2.1.2.1 + 4.2.1.2.2 + 4.2.1.2.3 = montant des opérations de paiement frauduleuses de 4.2.1.2; 4.2.1.3.1 + 4.2.1.3.2 + 4.2.1.3.3 = montant des opérations de paiement frauduleuses de 4.2.1.3; 4.2.2.2.1 + 4.2.2.2.2 + 4.2.2.2.3 =montant des opérations de paiement frauduleuses de4.2.2.2; 4.2.2.3.1 + 4.2.2.3.2 + 4.2.2.3.3 = montant des opérations de paiement frauduleuses de 4.2.2.3
4.2.1.2.1.1 + 4.2.1.2.1.2 + 4.2.1.2.1.3 + 4.2.1.2.1.4 + 4.2.1.2.1.5 = montant des opérations de paiement frauduleuses de 4.2.1.2.1; 4.2.1.3.1.1 + 4.2.1.3.1.2 + 4.2.1.3.1.3 + 4.2.1.3.1.4 + 4.2.1.3.1.5 = montant des opérations de paiement frauduleuses de 4.2.1.3.1; 4.2.2.2.1.1 + 4.2.2.2.1.2 + 4.2.2.2.1.3 + 4.2.2.2.1.4 = montant des opérations de paiement frauduleuses de4.2.2.2.1; 4.2.2.3.1.1 + 4.2.2.3.1.2 + 4.2.2.3.1.3 + 4.2.2.3.1.4 = montant des opérations de paiement frauduleuses de 4.2.2.3.1
► A1 4.2.1.3.4 + 4.2.1.3.5 + 4.2.1.3.6 + 4.2.1.3.7 + 4.2.1.3.8 = 4.2.1.3; 4.2.2.3.4 + 4.2.2.3.5+ 4.2.2.3.6 + 4.2.2.3.7 = 4.2.2.3

E- Ventilation des données pour les opérations de retrait d'espèces par carte devant être déclarées par le prestataire de services de paiement ► A1 émetteur

▼ A1

	Libellé	Opérations de paiement	Opérations de paiement frauduleuses
5	Retrait d'espèces	X	X
	<i>Dont ventilation par fonction de la carte:</i>		
5.1	Dont retraits d'espèces par carte dotée d'une fonction de débit	X	X
5.2	Dont retraits d'espèces par carte dotée d'une fonction de crédit ou de débit différé	X	X
	<i>dont retraits d'espèces frauduleux par type de fraude:</i>		
5.2.1	Émission d'un ordre de paiement (retrait d'espèces) par le fraudeur		X
5.2.1.1	Carte perdue ou volée		X
5.2.1.2	Carte non reçue		X
5.2.1.3	Carte contrefaite		X
5.2.1.4	Autres		X
5.2.2	Manipulation du payeur ayant pour effet d'obtenir un retrait d'espèces		X

Pertes dues à une fraude, par porteur de responsabilité:	Pertes totales
Le prestataire de services de paiement déclarant	X
L'utilisateur du service de paiement (titulaire du compte)	X
Autres	X

Validation

▼ A1

$5.1 + 5.2 = 5$
$5.3.1 + 5.3.2 = 5$
$5.3.1.1 + 5.3.1.2 + 5.3.1.3 + 5.3.1.4 = 5.3.1$

F- Ventilation des données à fournir pour les opérations de paiement en monnaie électronique

	Libellé	Opérations de paiement	Opérations de paiement frauduleuses
6	Opérations de paiement en monnaie électronique	X	X
6.1	Dont initiation via un canal de paiement distant	X	X
6.1.1	Dont opérations avec authentification client forte	X	X
	<i>dont les transactions frauduleuses payées en monnaie électronique par type de fraude:</i>		
6.1.1.1	Émission d'un ordre de paiement par le fraudeur		X
6.1.1.2	Modification d'un ordre de paiement par le fraudeur		X
6.1.1.3	Manipulation du payeur par le fraudeur ayant pour effet d'émettre un ordre de paiement		X
6.1.2	Dont opérations avec authentification client non forte	X	X
	<i>dont les transactions frauduleuses payées en monnaie électronique par type de fraude:</i>		
6.1.2.1	Émission d'un ordre de paiement par le fraudeur		X
6.1.2.2	Modification d'un ordre de paiement par le fraudeur		X
6.1.2.3	Manipulation du payeur par le fraudeur ayant pour effet d'émettre un ordre de paiement		X
	<i>dont ventilation par motif d'omission d'authentification client forte</i>		
6.1.2.4	Faible montant (article16 NTR)	X	X
6.1.2.5	Bénéficiaire de confiance (article13 NTR)	X	X
6.1.2.6	Opération récurrente (article14 NTR)	X	X
6.1.2.7	Paiement à soi-même (article15 NTR)	X	X
6.1.2.8	Utilisation de procédures et protocoles de paiement d'entreprise sécurisés (article 17 NTR)	X	X
6.1.2.9	Analyse des risques liés à l'opération (article18 NTR)	X	X

	Libellé	Opérations de paiement	Opérations de paiement frauduleuses
► A1 6.1.2.10	Opérations initiées par des commerçants ⁴	X	X
► A1 6.1.2.11	Autres	X	X
6.2	Dont initiation via un canal de paiement non distant	X	X
6.2.1	Dont opérations avec authentification client forte	X	X
	<i>dont les transactions frauduleuses payées en monnaie électronique par type de fraude :</i>		
6.2.1.1	Émission d'un ordre de paiement par le fraudeur		X
6.2.1.2	Modification d'un ordre de paiement par le fraudeur		X
6.2.1.3	Manipulation du payeur par le fraudeur ayant pour effet d'émettre un ordre de paiement		X
6.2.2	Dont opérations avec authentification client non forte	X	X
	<i>dont les transactions frauduleuses payées en monnaie électronique par type de fraude:</i>		
6.2.2.1	Émission d'un ordre de paiement par le fraudeur		X
6.2.2.2	Modification d'un ordre de paiement par le fraudeur		X
6.2.2.3	Manipulation du payeur par le fraudeur ayant pour effet d'émettre un ordre de paiement		X
	<i>dont ventilation par motif d'omission d'authentification client forte</i>		
6.2.2.4	Bénéficiaire de confiance (article13 NTR)	X	X
6.2.2.5	Opération récurrente (article14 NTR)	X	X
6.2.2.6	Paiement sans contact de faible montant (article16 NTR)	X	X
6.2.2.7	Automates de paiement des frais de transport et de parking (article 12 NTR)	X	X
► A1 6.2.2.8	Autres	X	X

⁴ ► A1 Voir la note de bas de page 4

Pertes dues à une fraude, par porteur de responsabilité :	Pertes totales
Le prestataire de services de paiement déclarant	X
L'utilisateur du service de paiement	X
Autres	X

Validation

$6.1 + 6.2 = 6$
$6.1.1 + 6.1.2 = 6.1$; $6.2.1 + 6.2.2 = 6.2$
$6.1.1.1 + 6.1.1.2 + 6.1.1.3 =$ montant des opérations de paiement frauduleuses de 6.1.1; $6.1.2.1 + 6.1.2.2 + 6.1.2.3 =$ chiffre d'opération de paiement frauduleuse de 6.1.2; $6.2.1.1 + 6.2.1.2 + 6.2.1.3 =$ montant des opérations de paiement frauduleuses de 6.2.1; $6.2.2.1 + 6.2.2.2 + 6.2.2.3 =$ montant des opérations de paiement frauduleuses de 6.2.2
► A1 $6.1.2.4 + 6.1.2.5 + 6.1.2.6 + 6.1.2.7 + 6.1.2.8 + 6.1.2.9 + 6.1.2.10 + 6.1.2.11 = 6.1.2$; $6.2.2.4 + 6.2.2.5 + 6.2.2.6 + 6.2.2.7 + 6.2.2.8 = 6.2.2$

G- Ventilation des données à fournir pour les opérations de paiement de transmission de fonds

	Libellé	Opérations de paiement	Opérations de paiement frauduleuses
7	Transmission de fonds	X	X

H- Ventilation des données pour les opérations de paiement initiées par des prestataires de services d'initiation de paiement

	Libellé	Opérations de paiement	Opérations de paiement frauduleuses
8	Opérations de paiement initiées par des prestataires de services d'initiation de paiements	X	X
8.1	Dont opérations initiées via un canal de paiement à distance	X	X
8.1.1	Dont opérations avec authentification client forte	X	X
8.1.2	Dont opérations avec authentification client non forte	X	X
8.2	Dont initiation via un canal de paiement non distant	X	X
8.2.1	Dont opérations avec authentification client forte	X	X
8.2.2	Dont opérations avec authentification client non forte	X	X
	dont ventilation par instrument de paiement		
8.3.1	Virements	X	X
8.3.2	Autres	X	X

Validation

$8.1 + 8.2 = 8$
$8.3.1 + 8.3.2 = 8$
$8.1.1 + 8.1.2 = 8.1$
$8.2.1 + 8.2.2 = 8.2$