EBA/GL/2017/10

19/12/2017

Orientations

sur la notification des incidents majeurs en vertu de la directive (UE) 2015/2366 (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° 1093/2010[1]. 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 19/02/2019. 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/2017/10». 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 découlent du mandat conféré à l'ABE en vertu de l'article 96, paragraphe 3, de 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) n° 1093/2010, et abrogeant la directive 2007/64/CE (DSP2).

6. Ces orientations spécifient, en particulier, les critères pour la classification des incidents opérationnels ou de sécurité majeurs par les prestataires de services de paiement ainsi que le format et les procédures que ces derniers devraient appliquer pour informer de ces incidents, comme le prévoit l'article 96, paragraphe 1 de la directive susmentionnée, l'autorité compétente dans l'État membre d'origine.

7. En outre, les présentes orientations traitent de la manière dont ces autorités compétentes devraient évaluer la pertinence de l'incident et les éléments des notifications d'incident qu'elles communiqueront, comme le prévoit l'article 96, paragraphe 2, de ladite directive, à d'autres autorités nationales.

8. De plus, les présentes orientations traitent également de la communication des détails importants des incidents notifiés à l'ABE et à la BCE, afin de favoriser une approche commune et cohérente.

Champ d'application

9. Les présentes orientations s'appliquent en rapport avec la classification et la notification des incidents opérationnels ou de sécurité majeurs, conformément à l'article 96 de la directive (UE) 2015/2366.

10. Les présentes orientations s'appliquent à tous les incidents couverts par la définition d'«incident opérationnel ou de sécurité majeur», qui englobe les événements externes et internes qui pourraient être malveillants ou accidentels.

11. Les présentes orientations s'appliquent également lorsque l'incident opérationnel ou de sécurité majeur trouve son origine en dehors de l'Union (par exemple, lorsqu'un incident trouve son origine au sein de l'entreprise mère ou au sein d'une filiale établie en dehors de l'Union) et affecte les services de paiement fournis par un prestataire de services de paiement situé dans l'Union soit directement (un service lié au paiement est exécuté par l'entreprise

affectée établie en dehors de l'Union) soit indirectement (la capacité du prestataire de services de paiement à poursuivre ses activités de paiement est compromise d'une quelconque autre manière en raison de l'incident).

Destinataires

12. La première série d'orientations (section 4) s'adresse aux prestataires de services de paiement, tels que définis à l'article 4, paragraphe 11, de la directive(UE) 2015/2366 et tels que visés à l'article 4, paragraphe 1, du règlement (UE) n° 1093/2010.

13. Les deuxième et troisième séries d'orientations (sections 5 et 6) s'adressent aux autorités compétentes telles que définies à l'article 4, paragraphe 2, point i), du règlement (UE) n° 1093/2010.

Définitions

14. Sauf indication contraire, les termes employés et définis dans la directive(UE) 2015/2366 revêtent la même signification dans les Orientations. En outre, aux fins des présentes orientations, les définitions suivantes s'appliquent:

Incident opérationnel ou de sécurité	Un événement unique ou une série d'événements liés non planifiés par le prestataire de services de paiement, qui a ou aura probablement une incidence négative sur l'intégrité, la disponibilité, la confidentialité, l'authenticité et/ou la continuité des services liés au paiement.
Intégrité	Propriété consistant à préserver l'exactitude et le caractère complet des informations et éléments (y compris les données).
Disponibilité	Propriété selon laquelle les services liés au paiement sont accessibles et utilisables par les utilisateurs de services de paiement.
Confidentialité	Propriété selon laquelle les informations ne sont pas mises à la disposition ni divulguées à des personnes, entités ou processus non autorisés.
Authenticité	Propriété selon laquelle une source est ce qu'elle déclare être.
Continuité	Propriété selon laquelle les processus, tâches et actifs d'une entreprise nécessaires à la prestation de services liés au paiement sont pleinement accessibles et fonctionnels à des niveaux pré-définis acceptables.
Services liés au paiement	Toute activité exercée à titre professionnel au sens de l'article 4, paragraphe 3, de la DSP2, et toutes les tâches de soutien technique nécessaires à l'exécution des services de paiement.

3. Mise en œuvre

Date d'entrée en application

15. Les présentes orientations sont applicables à compter du 13 janvier 2018.

4. Orientations à l'intention des prestataires de services de paiement sur la notification des incidents opérationnels ou de sécurité majeurs à l'autorité compétente dans l'État membre d'origine

Orientation 1: Classification en tant qu'incident majeur

1.1. Les prestataires de services de paiement devraient classer comme majeurs les incidents opérationnels ou de sécurité qui remplissent

a. un ou plusieurs critères au «niveau d'impact supérieur», ou

b. trois critères ou plus au «niveau d'impact inférieur»

comme le prévoit la l'Orientation 1.4 et suite à l'évaluation prévue dans les présentes orientations.

1.2. Les prestataires de services de paiement devraient évaluer un incident opérationnel ou de sécurité par rapport aux critères suivants et à leurs indicateurs fondamentaux:

i. Opérations affectées

Les prestataires de services de paiement devraient déterminer le montant total des opérations affectées, ainsi que le nombre de paiements compromis en pourcentage du volume habituel des opérations de paiement menées avec les services de paiement affectés.

ii. Utilisateurs de services de paiement affectés

Les prestataires de services de paiement devraient déterminer le nombre d'utilisateurs de services de paiement affectés en termes absolus et en pourcentage du nombre total d'utilisateurs de services de paiement.

iii. Interruption du service

Les prestataires de services de paiement devraient déterminer la durée pendant laquelle le service sera probablement indisponible pour l'utilisateur de services de paiement ou pendant laquelle l'ordre de paiement, au sens de l'article 4, paragraphe (13), de la DSP2, ne pourra pas être exécuté par le prestataire de services de paiement.

iv. Impact économique

Les prestataires de services de paiement devraient déterminer les coûts monétaires associés à l'incident de manière globale et prendre en compte le chiffre absolu et, le cas échéant, l'importance relative de ces coûts par rapport à la taille du prestataire de services de paiement (à savoir, par rapport aux fonds propres de catégorie 1 du prestataire de services de paiement).

v. Niveau élevé d'escalade interne

Les prestataires de services de paiement devraient déterminer si cet incident a été ou sera probablement notifié à leurs cadres supérieurs.

vi. Autres prestataires de services de paiement ou infrastructures pertinentes potentiellement affectés

Les prestataires de services de paiement devraient déterminer les implications systémiques que l'incident aura probablement, à savoir ses retombées potentielles, non seulement sur le prestataire de services de paiement initialement affecté, mais également sur les autres prestataires de services de paiement, infrastructures du marché financier et/ou systèmes de paiement par carte.

vii. Impact en termes de réputation

Les prestataires de services de paiement devraient déterminer dans quelle mesure l'incident peut porter atteinte à la confiance accordée par les utilisateurs au prestataire de services de paiement lui-même et, plus généralement, au service sous-jacent ou au marché dans son ensemble.

1.3. Les prestataires de services de paiement devraient calculer la valeur des indicateurs selon la méthodologie suivante:

i. Opérations affectées

En règle générale, les prestataires de services de paiement devraient considérer comme des «opérations affectées» toutes les opérations nationales et transfrontalières qui ont été ou seront probablement directement ou indirectement affectées par l'incident et, en particulier, les opérations qui n'ont pas pu être initiées ou traitées, celles pour lesquelles le contenu du message de paiement a été modifié et celles qui ont été frauduleusement ordonnées (que les fonds aient été récupérés ou non).

En outre, les prestataires de services de paiement devraient définir le volume habituel des opérations de paiement comme étant la moyenne journalière annuelle des opérations de paiement nationales et transfrontalières menées avec les services de paiement qui ont été affectés par l'incident, en prenant l'année précédente comme période de référence pour les calculs. Si les prestataires de services de paiement estiment que ce chiffre n'est pas représentatif (par exemple, en raison des variations saisonnières), ils devraient utiliser une autre mesure, plus représentative, et communiquer à l'autorité compétente la justification qui sous-tend cette approche dans le champ correspondant du modèle (voir Annexe 1).

ii. Utilisateurs de services de paiement affectés

Les prestataires de services de paiement devraient définir comme étant des «utilisateurs de services de paiement affectés» tous les clients (au niveau national ou à l'étranger, consommateurs ou entreprises) qui ont un contrat avec le prestataire de services de paiement affecté qui leur donne accès au service de paiement affecté, et qui ont subi ou subiront probablement les conséquences de l'incident. Les prestataires de services de paiement devraient avoir recours à des estimations basées sur l'activité passée pour déterminer le nombre d'utilisateurs de services de paiement qui ont pu utiliser le service de paiement tout au long de l'incident.

En cas de groupes, chaque prestataire de services de paiement devrait prendre en compte uniquement ses propres utilisateurs de services de paiement. Si un prestataire de services de paiement propose des services opérationnels à d'autres personnes, ce prestataire de services de paiement devrait prendre en compte uniquement ses propres utilisateurs de services de paiement (le cas échéant) et les prestataires de services de paiement bénéficiant de ces services opérationnels devraient évaluer l'incident en rapport avec leurs propres utilisateurs de services de paiement.

De plus, les prestataires de services de paiement devraient prendre comme nombre total d'utilisateurs de services de paiement le chiffre cumulé des utilisateurs de services de paiement nationaux et transfrontaliers avec lesquels ils sont contractuellement liés au moment de l'incident (sinon, le chiffre le plus récent disponible) et qui ont accès au service de paiement affecté, quelle que soit leur taille ou qu'ils soient considérés comme des utilisateurs de services de paiement actifs ou passifs.

iii. Interruption du service

Les prestataires de services de paiement devraient prendre en compte la durée pendant laquelle toute tâche, tout processus ou tout canal lié à la prestation de services de paiement est ou sera probablement interrompu et empêche ainsi (i) l'initiation et/ou l'exécution d'un service de paiement et/ou (ii) l'accès à un compte de paiement. Les prestataires de services de paiement devraient comptabiliser l'interruption de service à partir du moment où l'interruption se déclenche, et ils devraient prendre en compte les intervalles de temps au cours desquels ils sont opérationnels pour l'exécution de services de paiement ainsi que les heures de fermeture et les périodes de maintenance, le cas échéant et si applicable. Si les prestataires de services de paiement ne sont pas en mesure de déterminer le moment où l'interruption du service s'est déclenchée, ils devraient exceptionnellement comptabiliser l'interruption de service à partir du moment où l'interruption est détectée.

iv. Impact économique

Les prestataires de services de paiement devraient prendre en compte les coûts qui peuvent être directement liés à l'incident et ceux qui sont indirectement liés à l'incident. Les prestataires de services de paiement devraient, notamment, prendre en compte les fonds ou actifs expropriés, les coûts de remplacement du matériel informatique ou des logiciels, les autres coûts d'analyses judiciaires ou de réparation, les frais dus au non-

respect des obligations contractuelles, les sanctions, les engagements extérieurs et les pertes de recettes. En ce qui concerne les coûts indirects, les prestataires de services de paiement devraient prendre en compte uniquement ceux qui sont déjà connus ou fortement susceptibles de se matérialiser.

v. *Niveau élevé d'escalade interne*

Les prestataires de services de paiement devraient déterminer si, en raison de son incidence sur les services liés au paiement, le directeur des systèmes d'information (ou fonction similaire) a été ou sera probablement informé de l'incident en dehors de toute procédure de notification périodique et sur une base continue tout au long de l'incident. En outre, les prestataires de services de paiement devraient déterminer si, en raison de l'impact de l'incident sur les services liés au paiement, un mode de «crise» a été ou est susceptible d'être déclenché.

vi. *Autres prestataires de services de paiement ou infrastructures pertinentes potentiellement affectés*

Les prestataires de services de paiement devraient évaluer l'impact de l'incident sur le marché financier, entendu comme étant les infrastructures du marché financier et/ou les systèmes de paiement par carte qui les soutiennent et d'autres prestataires de services de paiement. Plus particulièrement, les prestataires de services de paiement devraient évaluer si l'incident a été ou sera probablement reproduit chez d'autres prestataires de services de paiement, s'il a affecté ou affectera probablement le bon fonctionnement des infrastructures du marché financier et s'il a compromis ou compromettra probablement le bon fonctionnement du système financier dans son ensemble. Les prestataires de services de paiement devraient tenir compte de diverses dimensions telles que celles de savoir si le composant/logiciel affecté est propriétaire ou généralement disponible, si le réseau compromis est interne ou externe et si le prestataire de services de paiement a cessé ou cessera probablement de s'acquitter de ses obligations au sein des infrastructures du marché financier dont il est membre.

vii. *Impact en termes de réputation*

Les prestataires de services de paiement devraient tenir compte du degré de visibilité que l'incident a, à leur connaissance, gagné ou gagnera probablement sur le marché. Plus particulièrement, les prestataires de services de paiement devraient tenir compte de la probabilité selon laquelle l'incident portera préjudice à la société comme bon indicateur de sa capacité à affecter leur réputation. Les prestataires de services de paiement devraient déterminer si (i) l'incident a affecté un processus visible et est, par conséquent, susceptible de recevoir ou a déjà bénéficié d'une couverture médiatique (en tenant compte non seulement des médias traditionnels, tels que la presse, mais également des blogs, réseaux sociaux, etc.), (ii) les obligations réglementaires ont été ou ne seront probablement pas respectées, (iii) les sanctions ont été ou seront probablement violées ou (iv) le même type d'incident s'est déjà produit.

1.4. Les prestataires de services de paiement devraient évaluer un incident en déterminant, pour chaque critère individuel, si les seuils pertinents du Tableau 1 sont ou seront probablement atteints avant la résolution de l'incident.

Tableau 1: Seuils

Critères	Niveau d'impact inférieur	Niveau d'impact supérieur
Opérations affectées	> 10 % du volume habituel des opérations du prestataire de services de paiement (en nombre d'opérations) **et** > 100 000 EUR	> 25 % du volume habituel des opérations du prestataire de services de paiement (en nombre d'opérations) **ou** > 5 millions EUR
Utilisateurs de services de paiement affectés	> 5 000 **et** > 10 % des utilisateurs de services de paiement du prestataire de services de paiement	> 50 000 **ou** > 25 % des utilisateurs de services de paiement du prestataire de services de paiement
Interruption du service	> 2 heures	Sans objet
Impact économique	Sans objet	> Max. (0,1 % des fonds propres de catégorie 1*, 200 000 EUR) **ou** > 5 millions EUR
Niveau élevé d'escalade interne	Oui	Oui, et un mode de «crise» (ou équivalent) est susceptible d'être déclenché
Autres prestataires de services de paiement ou infrastructures pertinentes potentiellement affectés	Oui	Sans objet
Impact en termes de réputation	Oui	Sans objet

*Fonds propres de catégorie 1 tels que définis à l'article 25 du règlement (UE) n° 575/2013 du Parlement européen et du Conseil du 26 juin 2013 concernant les exigences prudentielles applicables aux établissements de crédit et aux entreprises d'investissement et modifiant le règlement (UE) n° 648/2012.

1.5. Les prestataires de services de paiement devraient avoir recours à des estimations s'ils ne disposent pas de données réelles leur permettant de juger si un seuil donné a été ou sera probablement atteint avant la résolution de l'incident (par exemple, pendant la phase d'enquête initiale).

1.6. Les prestataires de services de paiement devraient mener cette évaluation sur une base continue tout au long de l'incident, pour identifier tout changement de statut éventuel, ascendant (de non majeur à majeur) ou descendant (de majeur à non majeur).

Orientation 2: Processus de notification

2.1. Les prestataires de services de paiement devraient recueillir toutes les informations pertinentes, rédiger une notification d'incident en utilisant le modèle prévu à l'Annexe 1 et

la soumettre à l'autorité compétente dans l'État membre d'origine. Les prestataires de services de paiement devraient compléter le modèle en suivant les instructions fournies à l'Annexe 1.

2.2. Les prestataires de services de paiement devraient utiliser le même modèle pour informer l'autorité compétente tout au long de l'incident (à savoir, pour les notifications initiale, intermédiaire et finale, telles que décrites aux paragraphes 2.7 à 2.21). Les prestataires de services de paiement devraient compléter le modèle de manière progressive, le mieux possible, au fur et à mesure que des informations supplémentaires sont facilement accessibles dans le cadre de leurs enquêtes internes.

2.3. Les prestataires de services de paiement devraient également présenter à l'autorité compétente dans leur État membre d'origine, le cas échéant, une copie des informations fournies (ou qui seront fournies) à leurs utilisateurs, comme le prévoit l'article 96, paragraphe 1, alinéa 2, de la DSP2, dès qu'elles sont disponibles.

2.4. Les prestataires de services de paiement devraient fournir à l'autorité compétente dans l'État membre d'origine, si elles sont disponibles et jugées pertinentes pour l'autorité compétente, toutes les informations supplémentaires en joignant une documentation supplémentaire au modèle standardisé sous forme d'une ou plusieurs annexes.

2.5. Les prestataires de services de paiement devraient assurer le suivi de toute demande de la part de l'autorité compétente dans l'État membre d'origine de fournir des informations ou clarifications complémentaires concernant la documentation déjà soumise.

2.6. Les prestataires de services de paiement devraient à tout moment préserver la confidentialité et l'intégrité des informations échangées avec l'autorité compétente dans leur État membre d'origine et également s'authentifier dûment auprès de l'autorité compétente dans leur État membre d'origine.

Notification initiale

2.7. Les prestataires de services de paiement devraient soumettre une notification initiale à l'autorité compétente dans l'État membre d'origine dès qu'un incident opérationnel ou de sécurité majeur est détecté pour la première fois.

2.8. Les prestataires de services de paiement devraient envoyer la notification initiale à l'autorité compétente dans les 4 heures suivant la détection de l'incident opérationnel ou de sécurité majeur, ou, s'il est connu que les canaux de notification de l'autorité compétente ne sont pas disponibles ou opérationnels à ce moment-là, dès qu'ils sont de nouveau disponibles/opérationnels.

2.9. Les prestataires de services de paiement devraient également soumettre une notification initiale à l'autorité compétente dans l'État membre d'origine lorsqu'un incident précédemment non majeur devient un incident majeur. Dans ce cas particulier, les

prestataires de services de paiement devraient envoyer la notification initiale à l'autorité compétente immédiatement après que le changement de statut a été identifié, ou, s'il est connu que les canaux de notification de l'autorité compétente ne sont pas disponibles ou opérationnels à ce moment-là, dès qu'ils sont de nouveau disponibles/opérationnels.

2.10. Les prestataires de services de paiement devraient inclure des informations globales (par exemple, section A du modèle) dans leurs notifications initiales, décrivant ainsi certaines caractéristiques fondamentales de l'incident et ses conséquences prévues sur la base des informations disponibles immédiatement après sa détection ou sa reclassification. Les prestataires de services de paiement devraient avoir recours à des estimations lorsque des données réelles ne sont pas disponibles. Les prestataires de services de paiement devraient également inclure dans leur notification initiale la date de la prochaine mise à jour, qui devrait être effectuée dans les plus brefs délais et en aucun cas au-delà de 3 jours ouvrables.

Notification intermédiaire

2.11. Les prestataires de services de paiement devraient soumettre des notifications intermédiaires chaque fois qu'ils considèrent qu'il y a une mise à jour pertinente du statut et, au minimum, à la date de la prochaine mise à jour indiquée dans la notification précédente (notification initiale ou notification intermédiaire).

2.12. Les prestataires de services de paiement devraient soumettre à l'autorité compétente une première notification intermédiaire contenant une description plus détaillée de l'incident et de ses conséquences (section B du modèle). De plus, les prestataires de services de paiement devraient produire des notifications intermédiaires supplémentaires en mettant à jour les informations déjà fournies aux sections A et B du modèle au moins, lorsqu'ils prennent connaissance de nouvelles informations pertinentes ou de changements significatifs depuis la précédente notification (par exemple, si l'incident s'est aggravé ou atténué, si de nouvelles causes ont été identifiées ou si des mesures ont été prises pour corriger le problème). Dans tous les cas, les prestataires de services de paiement devraient produire une notification intermédiaire à la demande de l'autorité compétente dans l'État membre d'origine.

2.13. Comme dans le cas des notifications initiales, si des données effectives ne sont pas disponibles, les prestataires de services de paiement devraient utiliser des estimations.

2.14. En outre, les prestataires de services de paiement devraient indiquer dans chaque notification la date de la prochaine mise à jour, qui devrait être effectuée dans les plus brefs délais et en aucun cas au-delà de 3 jours ouvrables. Si le prestataire de services de paiement n'est pas en mesure de respecter la date estimée pour la prochaine mise à jour, il devrait contacter l'autorité compétente afin d'expliquer les raisons de ce retard, de proposer une nouvelle date limite de soumission plausible (pas plus de 3 jours ouvrables) et envoyer une nouvelle notification intermédiaire mettant à jour exclusivement les informations concernant la date estimée de la prochaine mise à jour.

2.15. Les prestataires de services de paiement devraient envoyer la dernière notification intermédiaire lorsque les activités habituelles ont été rétablies et les affaires ont repris leur cours normal, en informant l'autorité compétente de cette situation. Les prestataires de services de paiement devraient considérer que l'activité est revenue à la normale lorsque les activités/opérations sont rétablies au même niveau de service/aux conditions tels que définis par le prestataire de services de paiement ou prévus en externe par un Contrat de niveau de service (CNS) en termes de délais de traitement, de capacité, d'exigences de sécurité, notamment, et lorsque les mesures d'urgence ne sont plus en place.

2.16. Si l'activité est revenue à la normale avant qu'un délai de 4 heures se soit écoulé depuis la détection de l'incident, les prestataires de services de paiement devraient s'efforcer de soumettre la notification initiale et la dernière notification intermédiaire simultanément (à savoir, compléter les sections A et B du modèle) avant l'expiration du délai de 4 heures.

Notification finale

2.17. Les prestataires de services de paiement devraient envoyer une notification finale lorsque l'analyse des causes profondes a été réalisée (sans tenir compte du fait que des mesures d'atténuation aient déjà été mises en œuvre ou non ou que la cause profonde finale ait été identifiée ou non) et lorsque des chiffres réels sont disponibles pour remplacer les estimations.

2.18. Les prestataires de services de paiement devraient remettre leur notification finale à l'autorité compétente dans un délai maximum de 2 semaines après que l'activité soit considérée comme revenue à la normale. Les prestataires de services de paiement qui ont besoin d'une extension de ce délai (par exemple, si aucun chiffre réel sur l'impact n'est encore disponible) devraient contacter l'autorité compétente avant l'expiration de ce délai et fournir une justification adéquate du retard, ainsi qu'une nouvelle date estimée pour la notification finale.

2.19. Si les prestataires de services de paiement sont en mesure de fournir toutes les informations requises dans notification finale (à savoir, la section C du modèle) dans le créneau de 4 heures suivant la détection de l'incident, ils devraient s'efforcer de soumettre dans leur notification initiale les informations liées aux notifications initiale, dernière intermédiaire et finale.

2.20. Les prestataires de services de paiement devraient s'efforcer d'inclure dans leurs notifications finales des informations complètes, à savoir (i) les chiffres réels sur l'impact au lieu d'estimations (ainsi que toute autre mise à jour nécessaire aux sections A et B du modèle) et (ii) la section C du modèle, qui comprend la cause profonde, si déjà connue, et un résumé des mesures adoptées ou devant être adoptées pour éliminer le problème et éviter qu'il ne se reproduise à l'avenir.

2.21. Les prestataires de services de paiement devraient également envoyer une notification finale lorsque, suite à l'évaluation continue de l'incident, ils identifient qu'un incident déjà

notifié ne remplit plus les critères pour être considéré comme majeur et ne devrait pas les remplir avant sa résolution. Dans ce cas, les prestataires de services de paiement devraient envoyer la notification finale dès que cette situation est détectée et, en tout cas, avant la date estimée de la prochaine notification. Dans ce cas particulier, au lieu de compléter la section C du modèle, les prestataires de services de paiement devraient cocher la case «incident reclassé comme non majeur» et expliquer les raisons justifiant ce déclassement.

Orientation 3: notification déléguée et consolidée

3.1. Lorsque l'autorité compétente le permet, les prestataires de services de paiement qui souhaitent déléguer les obligations de notification en vertu de la DSP2 à un tiers devraient en informer l'autorité compétente dans l'État membre d'origine et s'assurer que les conditions suivantes sont satisfaites:

a. Le contrat formel ou, le cas échéant, les dispositions internes existantes au sein d'un groupe, qui sous-tendent la notification déléguée entre le prestataire de services de paiement et le tiers, définissent sans ambiguïté l'attribution des responsabilités de l'ensemble des parties. En particulier, ils indiquent clairement que, indépendamment de la délégation éventuelle des obligations de notification, le prestataire de services de paiement affecté demeure pleinement responsable de la satisfaction des exigences énoncées à l'article 96 de la DSP2 et du contenu des informations fournies à l'autorité compétente dans l'État membre d'origine.

b. La délégation est conforme aux exigences en matière d'externalisation des fonctions opérationnelles importantes comme cela est prévu

i. à l'article 19, paragraphe 6, de la DSP2 concernant les établissements de paiement et les établissements de monnaie électronique, applicable mutatis mutandis conformément à l'article 3 de la directive 2009/110/CE (DME); ou

ii. dans les orientations du CECB relatives à l'externalisation concernant les établissements de crédit.

c. Les informations sont soumises à l'autorité compétente dans l'État membre d'origine au préalable et, en tout cas, en respectant tous les délais et procédures établis par l'autorité compétente, le cas échéant.

d. La confidentialité des données sensibles et la qualité, la cohérence, l'intégrité et la fiabilité des informations à fournir à l'autorité compétente sont dûment garanties.

3.2. Les prestataires de services de paiement qui souhaitent permettre au tiers désigné de remplir les obligations de notification de manière consolidée (à savoir, en présentant une seule notification se référant à plusieurs prestataires de services de paiement affectés par le même incident opérationnel ou de sécurité majeur) devraient informer l'autorité

compétente dans l'État membre d'origine, inclure les coordonnées figurant sous «PSP affecté» dans le modèle et s'assurer que les conditions suivantes sont satisfaites:

a. Inclure la présente disposition dans le contrat qui sous-tend la notification déléguée.

b. Soumettre la notification consolidée à la condition que l'incident soit occasionné par une perturbation des services fournis par le tiers.

c. Limiter la notification consolidée aux prestataires de services de paiement établis dans le même État membre.

d. S'assurer que le tiers évalue l'importance de l'incident pour chaque prestataire de services de paiement affecté et inclut dans la notification consolidée uniquement les prestataires de services de paiement pour lesquels l'incident est classé comme majeur. En outre, s'assurer, en cas de doute, qu'un prestataire de services de paiement est inclus dans la notification consolidée tant qu'il n'est pas prouvé qu'il ne devrait pas y figurer.

e. S'assurer, lorsque le modèle comprend des champs où une réponse commune n'est pas possible (par exemple, la section B 2, B 4 ou C 3), que le tiers (i) les complète individuellement pour chaque prestataire de services de paiement affecté, en précisant également l'identité de chaque prestataire de services de paiement auquel les informations se rapportent, ou (ii) utilise des fourchettes, dans les champs où cette option est proposée, représentant les valeurs les plus basses et les plus élevées telles qu'observées ou estimées pour les différents prestataires de services de paiement.

f. Les prestataires de services de paiement devraient s'assurer que le tiers leur communique à tout moment toutes les informations pertinentes concernant l'incident et toutes les interactions que le tiers peut avoir avec l'autorité compétente et leur contenu, mais uniquement dans la mesure où cela n'entraîne pas de violation de la confidentialité quant aux informations qui concernent d'autres prestataires de services de paiement.

3.3. Les prestataires de services de paiement ne devraient pas déléguer leurs obligations de notification avant d'informer l'autorité compétente dans l'État membre d'origine ou après avoir été informés de ce que le contrat d'externalisation ne répond pas aux exigences visées dans l'Orientation 3.1, lettre b).

3.4. Les prestataires de services de paiement qui souhaitent retirer la délégation de leurs obligations de notification devraient communiquer cette décision à l'autorité compétente dans l'État membre d'origine, en respectant les délais et procédures établis par cette dernière. Les prestataires de services de paiement devraient également informer l'autorité

compétente dans l'État membre d'origine de toute évolution importante affectant le tiers désigné et sa capacité à s'acquitter des obligations de notification.

3.5. Les prestataires de services de paiement devraient remplir matériellement leurs obligations de notification sans avoir recours à une assistance externe chaque fois que le tiers désigné omet d'informer l'autorité compétente dans l'État membre d'origine d'un incident opérationnel ou de sécurité majeur conformément à l'article 96 de la DSP2 et aux présentes orientations. En outre, les prestataires de services de paiement devraient veiller à ce qu'un incident ne soit pas notifié deux fois, individuellement par ledit prestataire de services de paiement et une nouvelle fois par le tiers.

Orientation 4: Politique opérationnelle et de sécurité

4.1. Les prestataires de services de paiement devraient s'assurer que leur politique opérationnelle et de sécurité générale définit clairement l'ensemble des responsabilités en matière de notification d'incidents en vertu de la DSP2, ainsi que les processus mis en œuvre pour satisfaire les exigences définies dans les présentes orientations.

5. Orientations à l'intention des autorités compétentes sur les critères d'évaluation de la pertinence de l'incident et les informations des notifications d'incidents à partager avec d'autres autorités nationales

Orientation 5: Évaluation de la pertinence de l'incident

5.1. Les autorités compétentes dans l'État membre d'origine devraient évaluer la pertinence d'un incident opérationnel ou de sécurité majeur pour les autres autorités nationales, en se fondant sur leur propre avis d'expert et en utilisant les critères suivants comme principaux indicateurs de l'importance dudit incident:

a. Les causes de l'incident relèvent de la compétence réglementaire de l'autre autorité nationale (à savoir, son domaine de compétence).
b. Les conséquences de l'incident ont un impact sur les objectifs d'une autre autorité nationale (par exemple, préservation de la stabilité financière).
c. L'incident affecte, ou pourrait affecter, des utilisateurs de services de paiement à grande échelle.
d. L'incident est susceptible de faire l'objet, ou a fait l'objet, d'une importante couverture médiatique.

5.2. Les autorités compétentes dans l'État membre d'origine devraient conduire cette évaluation sur une base continue tout au long de l'incident, pour identifier tout changement éventuel pouvant rendre important un incident qui n'était précédemment pas considéré comme tel.

Orientation 6: Informations à partager

6.1. Nonobstant toute autre obligation légale de partager des informations relatives à un incident avec d'autres autorités nationales, les autorités compétentes devraient fournir des informations au sujet d'incidents opérationnels ou de sécurité majeurs aux autorités nationales identifiées en suivant l'application de l'Orientation 5.1 (à savoir, «autres autorités nationales concernées»), au minimum, au moment de la réception de la notification initiale (ou de la notification ayant conduit au partage des informations) et lorsqu'il leur est notifié que les affaires ont repris leur cours normal (à savoir, la dernière notification intermédiaire).

6.2. Les autorités compétentes devraient soumettre à d'autres autorités nationales pertinentes les informations nécessaires pour offrir une vue d'ensemble clairement définie des événements et des conséquences potentielles. À cette fin, elles devraient fournir, au minimum, les informations données par le prestataire de services de paiement dans les champs suivants du modèle (dans la notification initiale ou intermédiaire):

- date et heure de détection de l'incident;
- date et heure de début de l'incident;
- date et heure auxquelles l'incident a été résolu ou devrait être résolu;
- description succincte de l'incident (y compris les parties non sensibles de la description détaillée);
- description succincte des mesures prises ou devant être prises en vue d'un rétablissement après l'incident;
- description de la manière dont l'incident pourrait affecter d'autres PSP et/ou infrastructures;
- description (le cas échéant) de la couverture médiatique;
- cause de l'incident.

6.3. Les autorités compétentes devraient procéder à une anonymisation appropriée, au besoin, et exclure toutes les informations pouvant être soumises à des restrictions de confidentialité ou de propriété intellectuelle avant de partager toute information relative à un incident avec d'autres autorités nationales pertinentes. Les autorités compétentes devraient, néanmoins, fournir aux autres autorités nationales pertinentes le nom et l'adresse du prestataire de services de paiement notifiant lorsque lesdites autorités nationales peuvent garantir que les informations seront traitées confidentiellement.

6.4. Les autorités compétentes devraient à tout moment préserver la confidentialité et l'intégrité des informations stockées et échangées avec les autres autorités nationales pertinentes et également s'authentifier correctement auprès des autres autorités nationales pertinentes. Plus particulièrement, les autorités compétentes devraient traiter toutes les informations reçues en vertu des présentes orientations conformément aux obligations de secret professionnel définies dans la DSP2, sans préjudice du droit de l'Union applicable et des exigences nationales.

6. Orientations à l'intention des autorités compétentes sur les critères d'évaluation des informations pertinentes des notifications d'incidents à partager avec l'ABE et la BCE et sur le format et les procédures de leur communication

Orientation 7: Informations à partager

7.1. Les autorités compétentes devraient toujours soumettre à l'ABE et à la BCE toutes les notifications reçues de (ou pour le compte de) prestataires de services de paiement affectés par un incident opérationnel ou de sécurité majeur (à savoir, notifications initiale, intermédiaire et finale).

Orientation 8: Communication

8.1. 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 également s'authentifier correctement auprès de l'ABE et de la BCE. Plus particulièrement, les autorités compétentes devraient traiter toutes les informations reçues en vertu des présentes orientations conformément aux obligations de secret professionnel définies dans la DSP2, sans préjudice du droit de l'Union applicable et des obligations nationales.

8.2. Pour éviter tout retard dans la transmission à l'ABE/la BCE d'informations relatives à un incident et permettre de minimiser les risques de perturbations opérationnelles, les autorités compétentes devraient encourager le recours à des moyens de communication appropriés.

Annexe 1 – Modèles de notification pour les prestataires de services de paiement

CLASSIFICATION: RESTRICTED

Major Incident Report

☐ Initial report	within 4 hours after detection
☐ Intermediate report	maximum of 3 business days from previous report
☐ Last intermediate report	
☐ Final report	within 2 weeks after closing the incident
☐ Incident reclassified as non-major — Please explain:	

Report date	DD/MM/YYYY	Time	HH:MM
Incident identification number, if applicable (for interim and final reports)			

A - Initial report

A 1 - GENERAL DETAILS					
Type of report					
Type of report	☐ Individual	☐ Consolidated			
Affected payment service provider (PSP)					
PSP name					
PSP unique identification number, if relevant					
PSP authorisation number					
Head of group, if applicable					
Home country					
Country/countries affected by the incident					
Primary contact person		Email		Telephone	
Secondary contact person		Email		Telephone	
Reporting entity (complete this section if the reporting entity is not the affected PSP in case of delegated reporting)					
Name of the reporting entity					
Unique identification number, if relevant					
Authorisation number, if applicable					
Primary contact person		Email		Telephone	
Secondary contact person		Email		Telephone	

A 2 - INCIDENT DETECTION and INITIAL CLASSIFICATION			
Date and time of detection of the incident	DD/MM/YYYY, HH:MM		
The incident was detected by (1)		If Other, please explain:	
Please provide a short and general description of the incident (should you deem the incident to have an impact in other EU Member States(s), and if feasible within the applicable reporting deadlines, please provide a translation in English)			
What is the estimated time for the next update?	DD/MM/YYYY, HH:MM		

B - Intermediate report

B 1 - GENERAL DETAILS

Please provide a more DETAILED description of the incident. e.g. information on: - What is the specific issue? - How it happened - How did it develop - Was it related to a previous incident? - Consequences (in particular for payment service users) - Background of the incident detection - Areas affected - Actions taken so far - Service providers/ third party affected or involved - Crisis management started (internal and/or external (Central Bank Crisis management)) - PSP internal classification of the incident	
Date and time of beginning of the incident (if already identified)	DD/MM/YYYY, HH:MM
Incident status	☐ Diagnostics ☐ Recovery ☐ Repair ☐ Restoration
Date and time when the incident was restored or is expected to be restored	DD/MM/YYYY, HH:MM

B 2 - INCIDENT CLASSIFICATION & INFORMATION ON THE INCIDENT

Overall impact	☐ Integrity ☐ Confidentiality ☐ Continuity ☐ Availability ☐ Authenticity
Transactions affected [2]	Number of transactions affected — ☐ Actual figure ☐ Estimation As a % of regular number of transactions — ☐ Actual figure ☐ Estimation Value of transactions affected in EUR — ☐ Actual figure ☐ Estimation Comments:
Payment service users affected [3]	Number of payment service users affected — ☐ Actual figure ☐ Estimation As a %-of total payment service users — ☐ Actual figure ☐ Estimation
Service downtime[4]	Total service downtime: DD:HH:MM — ☐ Actual figure ☐ Estimation
Economic impact [5]	Direct costs in EUR — ☐ Actual figure ☐ Estimation Indirect costs in EUR — ☐ Actual figure ☐ Estimation
High level of internal escalation	☐ YES ☐ YES, AND CRISIS MODE (OR EQUIVALENT) IS LIKELY TO BE CALLED UPON ☐ NO Describe the level of internal escalation of the incident, indicating if it has triggered or is likely to trigger a crisis mode (or equivalent) and if so, please describe
Other PSPs or relevant infrastructures potentially affected	☐ YES ☐ NO Describe how this incident could affect other PSPs and/or infrastructures
Reputational impact	☐ YES ☐ NO Describe how the incident could affect the reputation of the PSP (e.g. media coverage, potential legal or regulatory infringement, etc.)

B 3 - INCIDENT DESCRIPTION

Type of Incident	☐ Operational ☐ Security
Cause of incident	☐ Under investigation ☐ External attack ☐ Internal attack Type of attack: ☐ Distributed/Denial of Service (D/DoS) ☐ Infection of internal systems ☐ Targeted intrusion ☐ Other If Other, specify ☐ External events ☐ Human error ☐ Process failure ☐ System failure ☐ Other If Other, specify
Was the incident affecting you directly, or indirectly through a service provider?	☐ Directly ☐ Indirectly If indirectly, please provide the service provider's name

B 4 - INCIDENT IMPACT

Building(s) affected (Address), if applicable	
Commercial channels affected	☐ Branches ☐ Telephone banking ☐ Point of sale ☐ E-banking ☐ Mobile banking ☐ Other ☐ ATMs If Other, specify:
Payment services affected	☐ Cash placement on a payment account ☐ Credit transfers ☐ Money remittance ☐ Cash withdrawal from a payment account ☐ Direct debits ☐ Payment initiation services ☐ Operations required for operating a payment account ☐ Card payments ☐ Account information services ☐ Acquiring of payment instruments ☐ Issuing of payment instruments ☐ Other If Other, specify:
Functional areas affected	☐ Authentication/authorisation ☐ Clearing ☐ Indirect settlement ☐ Communication ☐ Direct settlement ☐ Other If Other, specify:
Systems and components affected	☐ Application/software ☐ Hardware ☐ Database ☐ Network/infrastructure ☐ Other If Other, specify:
Staff affected	☐ YES ☐ NO Describe how the incident could affect the staff of the PSP/service provider (e.g. staff not being able to reach the office to support customers, etc.)

B 5 - INCIDENT MITIGATION

Which actions/measures have been taken so far or are planned to recover from the incident?	
Has the Business Continuity Plan and/or Disaster Recovery Plan been activated? If so, when? If so, please describe	☐ YES ☐ NO DD/MM/YYYY, HH:MM
Has the PSP cancelled or weakened some controls because of the incident? If so, please explain	☐ YES ☐ NO

C - Final report	
If no intermediate report has been sent, please also complete section B	
C 1 - GENERAL DETAILS	
Please update the information from the intermediate report (summary): - additional actions/measures taken to recover from the incident - final remediation actions taken - root cause analysis - lessons learnt - addittional actions - any other relevant information	
Date and time of closing the incident	DD/MM/YYYY, HH:MM
If the PSP had to cancel or weaken some controls because of the incident, are the original controls back in place?	☐ YES ☐ NO
If so, please explain	
C 2 - ROOT CAUSE ANALYSIS AND FOLLOW-UP	
What was the root cause (if already known)? (possible to attach a file with detailed information)	
Main corrective actions/measures taken or planned to prevent the incident from happening again in the future, if already known	
C 3 - ADDITIONAL INFORMATION	
Has the incident been shared with other PSPs for information purposes?	☐ YES ☐ NO
If so, please provide details	
Has any legal action been taken against the PSP?	☐ YES ☐ NO
If so, please provide details	

Notes:

(1) Pull-down menu: payment service user; internal organisation; external organisation; none of the above

(2) Pull-down menu: > 10% of regular level of transactions and > EUR 100,000; > 25% of regular level of transactions or > EUR 5 milion; none of the above

(3) Pull-down menu: > 5,000 and > 10% payment service users; > 50,000 or > 25% payment service users; none of the above

(4) Pull-down menu: > 2 hours; < 2 hours

(5) Pull-down menu: > Max (0,1% Tier 1 capital, EUR 200,000) or > EUR 5 million; none of the above

CONSOLIDATED REPORT - LIST OF PSPs		
PSP Name	**PSP Unique Identification Number**	**PSP Authorisation number**

INSTRUCTIONS POUR COMPLÉTER LES MODÈLES

Les prestataires de services de paiement devraient compléter la section pertinente du modèle, en fonction de la phase de notification dans laquelle ils se trouvent: la section A pour la notification initiale, la section B pour les notifications intermédiaires et la section C pour la notification finale. Tous les champs sont obligatoires, sauf disposition clairement contraire.

Titre

Notification initiale: il s'agit de la première notification que le PSP soumet à l'autorité compétente dans l'État membre d'origine.

Notification intermédiaire: il s'agit d'une mise à jour d'une notification (initiale ou intermédiaire) précédente sur le même incident.

Dernière notification intermédiaire: elle informe l'autorité compétente dans l'État membre d'origine que les activités habituelles ont été rétablies et que les affaires ont repris leur cours normal. Aucune autre notification intermédiaire ne sera donc soumise.

Notification finale: il s'agit de la dernière notification que le PSP enverra sur l'incident, étant donné (i) qu'une analyse des causes profondes a déjà été réalisée et que les estimations peuvent être remplacées par des chiffres réels ou (ii) que l'incident n'est plus considéré comme un incident majeur.

Incident reclassé comme incident non majeur: l'incident ne remplit plus les critères pour être considéré comme un incident majeur et ne devrait pas les remplir avant qu'il soit résolu. Les PSP devraient expliquer les raisons de ce déclassement.

Date et heure de la notification: la date et l'heure exactes de soumission de la notification à l'autorité compétente.

Numéro d'identification de l'incident, le cas échéant (pour la notification intermédiaire et la notification finale): le numéro de référence délivré par l'autorité compétente au moment de la notification initiale pour identifier de manière unique l'incident, le cas échéant (à savoir, si une telle référence est fournie par l'autorité compétente).

A – Notification initiale

A 1 – Informations générales

Type de notification:

individuelle: la notification concerne un seul PSP.

consolidée: la notification concerne plusieurs PSP utilisant l'option de notification consolidée. Les champs sous «PSP affecté» devraient être laissés vierges (à l'exception du champ «Pays affecté(s) par l'incident» et une liste des PSP inclus dans la notification devrait être fournie en complétant le tableau correspondant (Notification consolidée – Liste des PSP).

PSP affecté: concerne le PSP qui subit l'incident.

Nom du PSP: le nom complet du PSP qui fait l'objet de la procédure de notification tel qu'il figure dans le registre PSP national officiel applicable.

Numéro d'identification unique du PSP, le cas échéant: le numéro d'identification unique correspondant utilisé dans chaque État membre pour identifier le PSP, qui doit être fourni par le PSP si le champ «Numéro d'autorisation du PSP» n'est pas complété.

Numéro d'autorisation du PSP: le numéro d'autorisation utilisé dans l'État membre d'origine.

Chef de groupe: en cas de groupes d'entités tels que définis à l'article 4, paragraphe 40, de 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) 1093/2010, et abrogeant la directive 2007/64/CE, veuillez indiquer le nom de l'entité de tête.

Pays d'origine: l'État membre dans lequel le siège statutaire du PSP est situé; ou si, conformément à son droit national, le prestataire de services de paiement n'a pas de siège statutaire, l'État membre dans lequel son administration centrale est située.

Pays affecté(s) par l'incident: le(s) pays où l'impact de l'incident s'est matérialisé (par exemple, plusieurs succursales d'un PSP situées dans différents pays sont affectées). Il peut s'agir ou non du même pays que l'État membre d'origine.

Personne de contact principale: le nom et le prénom de la personne chargée de notifier l'incident ou, si un tiers soumet la notification pour le compte du PSP affecté, le nom et le prénom de la personne responsable du service de gestion des incidents/des risques ou d'un domaine similaire, auprès du PSP affecté.

Adresse électronique: l'adresse électronique à laquelle toute demande de précisions peut être adressée, si nécessaire. Il peut s'agir d'une adresse électronique individuelle ou d'entreprise.

Téléphone: le numéro de téléphone à appeler pour toute demande de précisions, si nécessaire. Il peut s'agir d'un numéro de téléphone individuel ou d'entreprise.

Personne de contact secondaire: le nom et le prénom d'une autre personne qui peut être contactée par l'autorité compétente pour demander des informations sur un incident lorsque l'interlocuteur principal n'est pas disponible. Si un tiers soumet la notification pour le compte du PSP affecté, le nom et le prénom d'une autre personne au sein du service de gestion des incidents/des risques ou d'un domaine similaire, auprès du PSP affecté.

Adresse électronique: l'adresse électronique de l'autre interlocuteur à laquelle toute demande de précisions peut être envoyée, si nécessaire. Il peut s'agir d'une adresse électronique individuelle ou d'entreprise.

Téléphone: le numéro de téléphone de l'autre personne de contact à appeler pour toute demande de précisions, si nécessaire. Il peut s'agir d'un numéro de téléphone individuel ou d'entreprise.

Entité notifiante: cette section devrait être remplie si un tiers s'acquitte des obligations de notification pour le compte du PSP affecté.

Nom de l'entité notifiante: le nom complet de l'entité qui notifie l'incident, ainsi qu'il figure dans le registre commercial national officiel applicable.

Numéro d'identification unique, le cas échéant: le numéro d'identification unique correspondant utilisé dans le pays où le tiers est situé pour identifier l'entité qui notifie l'incident, qui doit être fourni par l'entité notifiante si le champ «Numéro d'autorisation» n'est pas complété.

Numéro d'autorisation, le cas échéant: le numéro d'autorisation du tiers dans le pays où il est situé, le cas échéant.

Personne de contact principale: le nom et le prénom de la personne chargée de notifier l'incident.

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

Téléphone: le numéro de téléphone à appeler pour toute demande de précisions, si nécessaire. Il peut s'agir d'un numéro de téléphone individuel ou d'entreprise.

Personne de contact secondaire: le nom et le prénom d'une autre personne au sein de l'entité qui notifie l'incident et qui peut être contactée par l'autorité compétente

lorsque la personne de contact principale n'est pas disponible.

Adresse électronique: l'adresse électronique de l'autre interlocuteur à laquelle toute demande de précisions peut être envoyée, si nécessaire. Il peut s'agir d'une adresse électronique individuelle ou d'entreprise.
Téléphone: le numéro de téléphone de l'autre personne de contact à appeler pour toute demande de précisions, si nécessaire. Il peut s'agir d'un numéro de téléphone individuel ou d'entreprise.

A 2 – Détection de l'incident et classification initiale

Date et heure de détection de l'incident: la date et l'heure auxquelles l'incident a été identifié pour la première fois.
Incident détecté par: indiquer si l'incident a été détecté par un utilisateur de services de paiement, une autre partie au sein du PSP (par exemple, fonction d'audit interne) ou par une partie externe (par exemple, prestataire de services externe). S'il ne s'agissait d'aucun de ceux-ci, veuillez fournir une explication dans le champ correspondant.
Description succincte et générale de l'incident: veuillez expliquer brièvement les problèmes les plus pertinents de l'incident, en précisant les causes possibles, les impacts immédiats, etc.
Quelles sont la date et l'heure estimées de la prochaine mise à jour?: indiquer la date et l'heure estimées pour la soumission de la prochaine mise à jour (notification intermédiaire ou finale).

B – Notification intermédiaire

B 1 – Informations générales

Description plus détaillée de l'incident: veuillez décrire les principales caractéristiques de l'incident, en précisant au moins les points figurant dans le questionnaire (le problème spécifique auquel le PSP est confronté, comment il a débuté et il a évolué, le lien possible avec un incident antérieur, les conséquences, notamment pour les utilisateurs de services de paiement, etc.).
Date et heure de début de l'incident: la date et l'heure auxquelles l'incident a débuté, si connues.
Statut de l'incident:

Diagnostics: les caractéristiques de l'incident viennent d'être identifiées.
Réparation: les éléments attaqués sont en cours de reconfiguration.
Reprise: les éléments défaillants sont en cours de rétablissement à leur dernier état récupérable.
Rétablissement: le service lié au paiement est de nouveau proposé.

Date et heure auxquelles l'incident a été résolu ou devrait être résolu: indiquer la date et l'heure auxquelles l'incident a été ou devrait être maîtrisé et l'activité a repris ou devrait redevenir normale.

B 2 – Classification de l'incident/Informations sur l'incident

Impact global: veuillez indiquer les dimensions qui ont été affectées par l'incident. Plusieurs cases peuvent être cochées.

Intégrité: la propriété consistant à préserver l'exactitude et le caractère complet des actifs (y compris les données).
Disponibilité: la propriété selon laquelle des services liés au paiement sont accessibles et utilisables par des utilisateurs de services de paiement.

Confidentialité: la propriété selon laquelle des informations ne sont pas mises à la disposition ni divulguées à des personnes, entités ou processus non autorisés.
Authenticité: la propriété selon laquelle une source est ce qu'elle déclare être.
Continuité: la propriété selon laquelle les processus, tâches et actifs d'une entreprise nécessaires à la prestation de services liés au paiement sont pleinement accessibles et fonctionnels à des niveaux prédéfinis acceptables.

Opérations affectées: Les PSP devraient indiquer les seuils qui ont été ou seront probablement atteints par l'incident, le cas échéant, et les chiffres correspondants: nombre d'opérations affectées, pourcentage d'opérations affectées par rapport au nombre d'opérations de paiement effectuées avec les services de paiement qui ont été affectés par l'incident, et montant total des opérations. Les PSP devraient fournir des valeurs spécifiques pour ces variables, qui peuvent être des chiffres effectifs ou des estimations. Les entités qui notifient pour le compte de plusieurs PSP (notification consolidée) peuvent fournir des fourchettes de valeurs à la place, qui représentent les valeurs les plus basses et les plus élevées observées ou estimées au sein du groupe de PSP inclus dans la notification, séparées par un trait d'union. En règle générale, les PSP devraient considérer comme des «opérations affectées» toutes les opérations nationales et transfrontalières qui ont été ou seront probablement directement ou indirectement affectées par l'incident et, en particulier, les opérations qui n'ont pas pu être initiées ou traitées, celles pour lesquelles le contenu du message de paiement a été modifié, et celles qui ont été frauduleusement ordonnées (que les fonds aient été récupérés ou non). En outre, les PSP devraient considérer le volume habituel des opérations de paiement comme étant la moyenne journalière annuelle des opérations de paiement nationales et transfrontalières menées avec les services de paiement qui ont été affectés par l'incident, en prenant l'année précédente comme période de référence pour les calculs. Si les PSP estiment que ce chiffre n'est pas représentatif (par exemple, en raison des variations saisonnières), ils devraient utiliser à la place une autre mesure plus représentative et communiquer à l'autorité compétente le motif qui sous-tend cette approche dans le champ «Commentaires».

Utilisateurs de services de paiement affectés: Les PSP devraient indiquer les seuils qui ont été ou seront probablement atteints par l'incident, le cas échéant, et les chiffres correspondants: nombre total d'utilisateurs de services de paiement affectés et pourcentage d'utilisateurs de services de paiement affectés par rapport au nombre total d'utilisateurs de services de paiement. Les PSP devraient fournir des valeurs concrètes pour ces variables, qui peuvent être des chiffres effectifs ou des estimations. Les entités qui notifient pour le compte de plusieurs PSP (notification consolidée) peuvent fournir des fourchettes de valeurs à la place, qui représentent les valeurs les plus basses et les plus élevées observées ou estimées au sein du groupe de PSP inclus dans la notification, séparées par un trait d'union. Les PSP devraient considérer comme des «utilisateurs de services de paiement affectés» tous les clients (nationaux ou étrangers, consommateurs ou entreprises) ayant un contrat avec le prestataire de services de paiement affecté qui leur donne accès au service de paiement affecté, et qui ont subi ou subiront probablement les conséquences de l'incident. Les PSP devraient avoir recours à des estimations basées sur l'activité antérieure pour déterminer le nombre d'utilisateurs de services de paiement qui ont pu utiliser le service de paiement tout au long de l'incident. En cas de groupes, chaque PSP devrait prendre en compte uniquement ses propres utilisateurs de services de paiement. Dans le cas d'un PSP qui propose des services opérationnels à d'autres personnes, ce PSP devrait prendre en compte uniquement ses propres utilisateurs de services de paiement (le cas échéant), et les PSP bénéficiant de ces services opérationnels devraient également évaluer l'incident en relation avec leurs propres utilisateurs de services de paiement. De plus, les PSP devraient prendre comme nombre total d'utilisateurs de services de paiement le chiffre cumulé des utilisateurs de services de paiement nationaux et transfrontaliers avec

lesquels ils sont contractuellement liés au moment de l'incident (ou le chiffre le plus récent disponible) et ayant accès au service de paiement affecté, quelle que soit leur taille ou qu'ils soient considérés comme des utilisateurs de services de paiement actifs ou passifs.

Interruption du service: Les PSP devraient indiquer si le seuil a été ou sera probablement atteint par l'incident et le chiffre correspondant: interruption totale du service. Les PSP devraient fournir des valeurs concrètes pour cette variable, qui peuvent être des chiffres effectifs ou des estimations. Les entités qui notifient pour le compte de plusieurs PSP (notification consolidée) peuvent fournir des fourchettes de valeurs à la place, représentant les valeurs les plus basses et les plus élevées observées ou estimées au sein du groupe de PSP inclus dans la notification, séparées par un trait d'union. Les PSP devraient prendre en compte la durée pendant laquelle tout tâche, tout processus ou tout canal lié à la prestation de services de paiement est ou sera probablement interrompu et empêche ainsi (i) l'initiation et/ou l'exécution d'un service de paiement et/ou (ii) l'accès à un compte de paiement. Les PSP devraient comptabiliser l'interruption de service à partir du moment où l'interruption se déclenche, et ils devraient prendre en compte les intervalles de temps au cours desquels ils sont opérationnels pour l'exécution de services de paiement ainsi que les heures de fermeture et les périodes de maintenance, le cas échéant et si applicable. Si les prestataires de services de paiement ne sont pas en mesure de déterminer le moment où l'interruption du service s'est déclenchée, ils devraient exceptionnellement comptabiliser l'interruption de service à partir du moment où l'interruption est détectée.

Impact économique: Les PSP devraient indiquer si le seuil a été ou sera probablement atteint par l'incident et les chiffres correspondants: coûts directs et coûts indirects. Les PSP devraient fournir des valeurs concrètes pour ces variables, qui peuvent être des chiffres effectifs ou des estimations. Les entités qui notifient pour le compte de plusieurs PSP (notification consolidée) peuvent fournir des fourchettes de valeurs à la place, représentant les valeurs les plus basses et les plus élevées observées ou estimées au sein du groupe de PSP inclus dans la notification, séparées par un trait d'union. Les PSP devraient prendre en compte les coûts qui peuvent être liés directement à l'incident et ceux qui sont indirectement liés à l'incident. Les PSP devraient, notamment, prendre en compte les fonds ou actifs expropriés, les coûts de remplacement de matériel informatique ou de logiciels, les autres coûts d'analyses judiciaires ou de réparation, les frais dus au non-respect des obligations contractuelles, les sanctions, les engagements extérieurs et les pertes de recettes. En ce qui concerne les coûts indirects, les PSP devraient prendre en compte uniquement ceux qui sont déjà connus ou fortement susceptibles de se matérialiser.

> **Coûts directs:** le montant (euros) directement imputable à l'incident, y compris les fonds nécessaires pour remédier à l'incident (par exemple, fonds ou actifs expropriés, coûts de remplacement du matériel informatique et des logiciels, frais résultant du non-respect des obligations contractuelles).
>
> **Coûts indirects:** le montant (euros) indirectement imputable à l'incident (par exemple, frais de réparation/indemnisation pour les clients, revenus perdus en raison d'opportunités commerciales manquées, frais juridiques éventuels).

Niveau élevé d'escalade interne: Les PSP devraient déterminer si, en raison de son incidence sur les services liés au paiement, le directeur des systèmes d'information (ou fonction similaire) a été ou sera probablement informé de l'incident en dehors de toute procédure de notification périodique et sur une base continue tout au long de l'incident. En cas de notification déléguée, l'escalade aurait lieu au sein du tiers. En outre, les PSP devraient déterminer si, en raison de l'impact de l'incident sur les services liés au paiement, un mode de «crise» a été ou est susceptible d'être déclenché ou non.

Autres PSP ou infrastructures pertinentes potentiellement affectés: les prestataires de services de paiement devraient évaluer l'impact de l'incident sur le marché financier, entendu comme étant les infrastructures du marché financier et/ou les systèmes de paiement par carte qui les soutiennent et d'autres PSP. Plus particulièrement, les PSP devraient évaluer si l'incident a été ou sera probablement reproduit chez d'autres PSP, s'il a affecté ou affectera probablement le bon fonctionnement des infrastructures du marché financier et s'il a compromis ou compromettra probablement la solidité du système financier dans son ensemble. Les PSP devraient tenir compte de diverses dimensions telles que celles de savoir si le composant/logiciel affecté est propriétaire ou généralement disponible, si le réseau compromis est interne ou externe et si le PSP a cessé ou cessera probablement de s'acquitter de ses obligations au sein des infrastructures du marché financier dont il est membre.

Impact en termes de réputation: Les PSP devraient tenir compte du degré de visibilité que l'incident a, à leur connaissance, gagné ou gagnera probablement sur le marché. Plus particulièrement, les PSP devraient tenir compte de la probabilité selon laquelle l'incident portera préjudice à la société comme bon indicateur de sa capacité à affecter leur réputation. Les PSP devraient déterminer si (i) l'incident a affecté ou non un processus visible et est, par conséquent, susceptible de recevoir ou a déjà bénéficié d'une couverture médiatique (en tenant compte non seulement des médias traditionnels, tels que la presse, mais également des blogs, réseaux sociaux, etc.), (ii) les obligations réglementaires ont été ou ne seront probablement pas respectées, (iii) les sanctions ont été ou seront probablement violées ou (iv) le même type d'incident s'est déjà produit.

B 3 – Description de l'incident

Type d'incident: indiquer si, à votre connaissance, il s'agit d'un incident opérationnel ou de sécurité.

Opérationnel: incident découlant de processus, personnes et systèmes inadéquats ou défaillants ou d'événements de force majeure qui affectent l'intégrité, la disponibilité, la confidentialité, l'authenticité et/ou la continuité de services liés au paiement.

Sécurité: accès non autorisé, utilisation, divulgation, perturbation, modification ou destruction des actifs du PSP qui affecte l'intégrité, la disponibilité, la confidentialité, l'authenticité et/ou la continuité de services liés au paiement. Ceci peut se produire lorsque, entre autres, le PSP fait l'objet de cyber-attaques, d'une conception ou mise en œuvre inadéquate des politiques de sécurité ou d'une sécurité physique inadéquate.

Cause de l'incident: indiquer la cause de l'incident ou, si elle n'est pas encore connue, celle qui est la plus probable. Plusieurs cases peuvent être cochées.

En cours d'enquête: la cause n'a pas encore été déterminée.

Attaque externe: la source de la cause vient de l'extérieur et cible intentionnellement le PSP (par exemple, attaques par des logiciels malveillants).

Attaque interne: la source de la cause vient de l'intérieur, et cible intentionnellement le PSP (par exemple, fraude interne).

Type d'attaque:

Déni de Service /distribué (D/DoS): une tentative ayant pour but de rendre un service en ligne indisponible en l'inondant d'un trafic provenant de sources multiples.

Infection des systèmes internes: une activité nuisible qui attaque les systèmes informatiques, en essayant de dérober de l'espace sur le disque dur ou du temps d'utilisation du processeur, d'accéder à des informations privées, de corrompre

des données, de polluposter des contacts, etc.

Intrusion ciblée: un acte non autorisé consistant à espionner, épier ou dérober des informations à travers le cyber-espace.

Autre: tout autre type d'attaque que le PSP peut avoir subie, directement ou par l'intermédiaire d'un prestataire de services. Plus particulièrement, en cas d'attaque visant le processus d'autorisation et d'authentification, cette case devrait être cochée. Des informations détaillées devraient être ajoutées dans le champ à texte libre.

Événements externes: la cause est associée à des événements échappant généralement au contrôle de l'entreprise (par exemple, catastrophes naturelles, problèmes juridiques, problèmes commerciaux et dépendances à l'égard de services).

Erreur humaine: l'incident a été causé par l'erreur involontaire d'une personne, que ce soit dans le cadre de la procédure de paiement (par exemple, téléchargement du mauvais fichier de lots de paiements sur le système de paiements) ou qu'elle y soit liée d'une manière ou d'une autre (par exemple, l'alimentation est coupée accidentellement et l'activité de paiement est mise en suspens).

Défaillance des processus: la cause de l'incident était une mauvaise conception ou exécution du processus de paiement, des contrôles des processus et/ou des processus de soutien (par exemple, processus de changement/migration, tests, configuration, capacité, surveillance).

Défaillance des systèmes: la cause de l'incident est associée à une inadéquation de la conception, de l'exécution, des composants, des spécifications, de l'intégration ou de la complexité des systèmes soutenant l'activité de paiement.

Autre: la cause de l'incident ne fait pas partie des causes ci-dessus. Des informations complémentaires devraient être fournies dans le champ à texte libre.

L'incident vous a-t-il affecté directement, ou indirectement par l'intermédiaire d'un prestataire de services?: un incident peut cibler un PSP directement ou l'affecter indirectement, par l'intermédiaire d'un tiers. En cas d'impact indirect, veuillez fournir le nom du ou des prestataires de services.

B 4 – Impact de l'incident

Bâtiment(s) affecté(s) (Adresse), le cas échéant: si un bâtiment physique est affecté, veuillez indiquer son adresse.

Canaux commerciaux affectés: veuillez indiquer le canal ou les canaux d'interaction avec les utilisateurs de services de paiement qui ont été affectés par l'incident. Plusieurs cases peuvent être cochées.

Succursales: lieu d'activité (autre que le siège social) qui fait partie d'un PSP, n'a aucune personnalité juridique et mène directement une partie ou la totalité des opérations inhérentes aux activités d'un PSP. Tous les sièges d'exploitation créés dans le même État membre par un PSP qui a son administration centrale dans un autre État membre devraient être considérés comme une seule succursale.

Services bancaires électroniques: l'utilisation d'ordinateurs pour exécuter des opérations financières sur l'internet.

Services bancaires par téléphone: l'utilisation de téléphones pour exécuter des opérations financières.

Services bancaires mobiles: l'utilisation d'une application bancaire spécifique sur un smartphone ou appareil similaire pour exécuter des opérations financières.

Distributeurs automatiques de billets: des appareils électromécaniques qui permettent aux utilisateurs de services de paiement de retirer des espèces de leurs comptes et/ou d'accéder à d'autres services.

Point de vente: les locaux physiques du commerçant chez lequel l'opération de paiement est initiée.

Autre: le canal commercial affecté ne fait pas partie des catégories ci-dessus. Des informations complémentaires devraient être fournies dans le champ à texte libre.

Services de paiement affectés: veuillez indiquer les services de paiement qui ne fonctionnent pas correctement suite à l'incident. Plusieurs cases peuvent être cochées.

Dépôt d'espèces sur un compte de paiement: la remise d'espèces à un PSP pour les créditer sur un compte de paiement.

Retrait d'espèces d'un compte de paiement: la demande reçue par un PSP de la part de son utilisateur de services de paiement pour fournir des espèces et débiter son compte de paiement du montant correspondant.

Mesures requises pour exploiter un compte de paiement: les actions devant être exécutées sur un compte de paiement pour l'activer, le désactiver et/ou le conserver (par exemple, ouverture, blocage).

Acquisition d'instruments de paiement: un service de paiement qui consiste à ce qu'un PSP passe un contrat avec un bénéficiaire visant à accepter et traiter des opérations de paiement, se traduisant par un transfert de fonds au bénéficiaire.

Virements: un service de paiement visant à créditer le compte de paiement d'un bénéficiaire d'une opération de paiement ou d'une série d'opérations de paiement depuis le compte de paiement d'un payeur par le PSP qui détient le compte de paiement du payeur, sur instruction du payeur.

Prélèvements: un service de paiement visant à débiter le compte de paiement d'un payeur, lorsqu'une opération de paiement est initiée par le bénéficiaire sur la base du consentement donné par le payeur au bénéficiaire, au prestataire de services de paiement du bénéficiaire ou au propre prestataire de services de paiement du payeur.

Paiements par carte: un service de paiement basé sur l'infrastructure et les règles commerciales du système de carte de paiement visant à effectuer une opération de paiement au moyen d'une carte, d'un appareil de télécommunication, numérique ou informatique, ou d'un logiciel s'il en résulte une opération par carte de débit ou crédit. Les opérations de paiement par carte excluent les opérations basées sur d'autres types de services de paiement.

Émission d'instruments de paiement: un service de paiement qui consiste pour un PSP qui passe un contrat avec un payeur à lui fournir un instrument de paiement pour initier et traiter les opérations de paiement du payeur.

Transmission de fonds: un service de paiement par lequel les fonds sont reçus d'un payeur, sans qu'aucun compte de paiement ne soit créé au nom du payeur ou du bénéficiaire, aux seules fins de transférer un montant correspondant à un bénéficiaire ou à un autre PSP agissant pour le compte du bénéficiaire, et/ou par lequel ces fonds sont reçus pour le compte et mis à la disposition du bénéficiaire.

Services d'initiation de paiement: des services de paiement visant à initier un ordre de paiement à la demande de l'utilisateur de services de paiement à l'égard d'un compte de paiement détenu chez un autre PSP.

Services d'information sur les comptes: des services de paiement en ligne visant à fournir des informations consolidées sur un ou plusieurs comptes de paiement détenus par l'utilisateur de services de paiement chez un autre PSP ou plusieurs PSP.

Autre: le service de paiement affecté ne fait pas partie des catégories ci-dessus. Des

informations complémentaires devraient être fournies dans le champ à texte libre.

Domaines fonctionnels affectés: veuillez indiquer l'étape ou les étapes du processus de paiement qui ont été affectées par l'incident. Plusieurs cases peuvent être cochées.

Authentification/autorisation: des procédures qui permettent au PSP de vérifier l'identité d'un utilisateur de services de paiement ou la validité de l'utilisation d'un instrument de paiement spécifique, y compris l'utilisation des données de sécurité personnalisées de l'utilisateur et le consentement donné par l'utilisateur de services de paiement (ou un tiers agissant pour le compte de cet utilisateur) pour transférer les fonds ou valeurs mobilières.

Communication: le flux d'informations à des fins d'identification, d'authentification, de notification et d'information entre le PSP gestionnaire du compte et les prestataires de services d'initiation de paiement, les prestataires de services d'information sur les comptes, les payeurs, les bénéficiaires et autres PSP.

Compensation: un processus consistant à transmettre, rapprocher et, dans certains cas, confirmer des ordres de transfert avant le règlement, comprenant éventuellement la compensation d'ordres et l'établissement de positions finales pour règlement.

Règlement direct: l'exécution d'une opération ou d'un traitement dans le but de permettre aux participants de s'acquitter de leurs obligations par le biais du transfert de fonds, lorsque cette action est réalisée par le PSP affecté lui-même.

Règlement indirect: la finalisation d'une opération ou d'un traitement dans le but de permettre aux participants de s'acquitter de leurs obligations par le biais du transfert de fonds, lorsque cette action est réalisée par un autre PSP pour le compte du PSP affecté.

Autre: le domaine fonctionnel affecté ne fait pas partie des catégories ci-dessus. Des informations complémentaires devraient être fournies dans le champ à texte libre.

Systèmes et composants affectés: indiquer quelle(s) partie(s) de l'infrastructure technologique du PSP a ou ont été affectée(s) par l'incident. Plusieurs cases peuvent être cochées.

Application/logiciel: les programmes, systèmes d'exploitation, etc. qui soutiennent la prestation de services de paiement par le PSP.

Base de données: la structure de données qui stocke les informations personnelles et de paiement nécessaires à l'exécution d'opérations de paiement.

Matériel informatique: l'équipement technologique physique qui exécute les processus et/ou stocke les données nécessaires aux PSP pour mener leurs activités liées au paiement.

Réseau/infrastructure: les réseaux de télécommunications, publics ou privés, qui permettent l'échange de données et d'informations au cours du processus de paiement (par exemple, l'internet).

Autre: le système et le composant affectés ne font pas partie des catégories ci-dessus. Des informations complémentaires devraient être fournies dans le champ à texte libre.

Personnel affecté: veuillez indiquer si l'incident a eu des répercussions sur le personnel du PSP et, dans l'affirmative, fournir des informations détaillées dans le champ à texte libre.

B 5 – Atténuation de l'incident

Quelles sont les actions/mesures qui ont été prises jusqu'à présent ou sont prévues pour remédier à l'incident?: veuillez fournir des informations détaillées sur les actions qui ont été prises ou sont prévues pour traiter temporairement l'incident.

Les plans de continuité des activités et/ou les plans de reprise après sinistre ont-ils été activés?: veuillez indiquer si oui ou non et, dans l'affirmative, fournir les informations les plus

pertinentes sur ce qui s'est passé (à savoir, quand ils ont été activés et en quoi consistaient ces plans).

Le PSP a-t-il annulé ou affaibli certains contrôles en raison de l'incident?: veuillez indiquer si le PSP a dû passer outre certains contrôles (par exemple, cesser d'appliquer le principe du double contrôle) pour traiter l'incident et, dans l'affirmative, fournir des informations détaillées sur les raisons qui sous-tendent l'affaiblissement ou l'annulation des contrôles.

C – Notification finale

C 1 – Informations générales

Mise à jour des informations à partir de la notification intermédiaire (résumé): veuillez fournir des informations complémentaires sur les actions prises pour remédier à l'incident et pour éviter qu'il ne se reproduise, l'analyse de la cause profonde, les enseignements tirés, etc.

Date et heure de clôture de l'incident: veuillez indiquer la date et l'heure auxquelles l'incident a été considéré clos.

Les contrôles d'origine sont-ils de nouveau en place?: si le PSP a dû annuler ou affaiblir certains contrôles en raison de l'incident, indiquer si ces contrôles sont de nouveau en place et fournir toute information complémentaire dans le champ à texte libre.

C 2 – Analyse des causes profondes et suivi

Quelle était la cause profonde, si déjà connue?: veuillez expliquer quelle est la cause profonde de l'incident ou, si elle n'est pas encore connue, quelles sont les conclusions préliminaires tirées de l'analyse des causes profondes. Les PSP peuvent joindre un fichier contenant des informations détaillées si jugé nécessaire.

Principales actions/mesures correctives prises ou prévues pour éviter que l'incident ne se reproduise à l'avenir, si déjà connues: veuillez décrire les principales actions qui ont été prises ou ont été prévues pour éviter que l'incident ne se reproduise à l'avenir.

C 3 – Informations supplémentaires

L'incident a-t-il été partagé avec d'autres PSP à titre d'information?: veuillez fournir une vue d'ensemble des PSP qui ont été contactés, de manière formelle ou informelle, pour les informer de l'incident, en fournissant des détails sur les PSP qui ont été informés, les informations qui ont été partagées et les raisons qui sous-tendent le partage de ces informations.

Une action en justice a-t-elle été intentée contre le PSP?: veuillez indiquer si, au moment de compléter le rapport final, le PSP a fait l'objet d'une action en justice (par exemple, s'il a été traduit devant les tribunaux ou s'il a perdu sa licence) suite à l'incident.