EBA/GL/2021/03

10 juin 2021

Orientations révisées

sur la notification des incidents majeurs en vertu de la DSP2

1. Obligations de conformité et de déclaration

Statut des présentes orientations

1. Le présent document contient des orientations formulées en vertu de l'article 16 du règlement instituant l'ABE[1]. Conformément à l'article 16, paragraphe 3, du règlement instituant l'ABE, 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 instituant l'ABE, 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 en priorité à des établissements.

Obligations de déclaration

3. Conformément à l'article 16, paragraphe 3, du règlement instituant l'ABE, les autorités compétentes doivent faire savoir avant le (07.11.2021) à l'ABE si elles respectent ou entendent respecter ces orientations ou communiquent, dans le cas contraire, les motifs de leur non-respect. En l'absence de toute 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 l'aide du formulaire disponible sur le site internet de l'ABE en indiquant en objet «EBA/GL/2021/03». Les notifications doivent être communiquées par des personnes dûment habilitées à rendre compte du respect des orientations au nom de leurs autorités compétentes. Tout changement en matière de conformité avec les orientations doit être signalé 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) nº 1093/2010 du Parlement européen et du Conseil du 24 novembre 2010 instituant une Autorité européenne de surveillance (Autorité bancaire européenne), modifiant la décision nº 716/2009/CE et abrogeant la décision 2009/78/CE de la Commission (JO L 331 du 15.12.2010, p. 12).

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) nº 1093/2010, et abrogeant la directive 2007/64/CE (DSP2).

6. Ces orientations spécifient, en particulier, les critères pour la classification des incidents majeurs opérationnels ou de sécurité par les prestataires de services de paiement ainsi que le format et les procédures que ces derniers doivent appliquer pour informer de ces incidents, comme le prévoit l'article 96, paragraphe 1, de la DSP2, l'autorité compétente dans l'État membre d'origine.

7. En outre, les présentes orientations traitent de la manière dont ces autorités compétentes doivent 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 la DSP2, à d'autres autorités nationales.

8. De plus, les présentes orientations traitent également de la communication des détails pertinents 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 majeurs opérationnels ou de sécurité, conformément à l'article 96 de la DSP2.

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

11. Les présentes orientations s'appliquent également lorsque l'incident majeur opérationnel ou de sécurité 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).

12. Les présentes orientations s'appliquent également aux incidents majeurs affectant des fonctions externalisées à des tiers par des prestataires de services de paiement.

Destinataires

13. 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 DSP2 et tels que visés à l'article 4, paragraphe 1, du règlement (UE) n° 1093/2010.

14. 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) nº 1093/2010.

Définitions

15. Sauf indication contraire, les termes employés et définis dans la DSP2 ont la même signification dans les orientations. En outre, aux fins des présentes orientations, on entend par:

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 et/ou l'authenticité 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 pleinement accessibles et utilisables par des utilisateurs de services de paiement, selon des niveaux acceptables prédéfinis par le prestataire 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.
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'application

16. Les présentes orientations s'appliquent à compter du 1er janvier 2022.

Abrogation

17. Les orientations suivantes sont abrogées à compter du 1er janvier 2022:

Orientations sur la notification des incidents majeurs en vertu de la directive (UE) 2015/2366 (DSP2) (EBA/GL/2017/10)

4. Orientations à l'intention des prestataires de services de paiement sur la notification des incidents opérationnels ou de sécurité 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 doivent 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 l'orientation 1.4 et suite à l'évaluation prévue dans les présentes orientations.

1.2. Les prestataires de services de paiement doivent 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. Atteinte à la sécurité des réseaux ou des systèmes d'information

Les prestataires de services de paiement devraient déterminer si une action malveillante a compromis la sécurité des réseaux ou des systèmes d'information liés à la fourniture de services de paiement.

iv. 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.

v. 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).

vi. 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.

vii. 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 est susceptible d'entraîner, 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.

viii. 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 doivent calculer la valeur des indicateurs selon la méthodologie suivante:

i. Opérations affectées:

En règle générale, les prestataires de services de paiement doivent 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 ordonnées frauduleusement (que les fonds aient été récupérés ou non) ou dont la bonne exécution est empêchée ou entravée de toute autre manière par l'incident.

Pour les incidents opérationnels ayant un impact sur la capacité d'initier et/ou de traiter des opérations, les prestataires de services de paiement ne doivent notifier que les incidents d'une durée supérieure à une heure. La durée de l'incident doit être mesurée à partir du moment où l'incident survient jusqu'au moment où les activités/opérations habituelles sont rétablies au niveau de service qui était assuré avant l'incident.

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 doivent 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 l'annexe).

ii. Utilisateurs de services de paiement affectés

Les prestataires de services de paiement doivent 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 doivent 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 doit 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 doit 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 doivent évaluer l'incident en rapport avec leurs propres utilisateurs de services de paiement.

Pour les incidents opérationnels ayant un impact sur la capacité d'initier et/ou de traiter des opérations, les prestataires de services de paiement ne doivent notifier que les incidents qui affectent les utilisateurs de services de paiement pendant une durée supérieure à une heure. La durée de l'incident doit être mesurée à partir du moment où l'incident survient jusqu'au moment où les activités/opérations habituelles sont rétablies au niveau de service qui était assuré avant l'incident.

De plus, les prestataires de services de paiement doivent 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. Atteinte à la sécurité des réseaux ou des systèmes d'information

Les prestataires de services de paiement doivent déterminer si une action malveillante a compromis la disponibilité, l'authenticité, l'intégrité ou la confidentialité des réseaux ou des systèmes d'information (y compris les données) liés à la fourniture de services de paiement.

iv. Interruption du service

Les prestataires de services de paiement doivent 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 doivent comptabiliser l'interruption de service à partir du moment où l'interruption se déclenche, et ils doivent 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 doivent exceptionnellement comptabiliser l'interruption de service à partir du moment où l'interruption est détectée.

v. Impact économique

Les prestataires de services de paiement doivent 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 doivent, notamment, prendre en compte les fonds ou actifs expropriés, les coûts de remplacement du matériel informatique ou des logiciels, les autres coûts d'analyses ou de remédiation, 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 doivent prendre en compte uniquement ceux qui sont déjà connus ou fortement susceptibles de se matérialiser.

vi. *Niveau élevé d'escalade interne*

Les prestataires de services de paiement doivent déterminer si, en raison de l'impact sur les services liés au paiement, l'organe de direction, tel que défini par les orientations de l'ABE sur la gestion des risques liés aux TIC et à la sécurité, a été ou sera probablement informé de l'incident, conformément à l'orientation 60 d) des orientations de l'ABE sur la gestion des risques liés aux TIC et à la sécurité, 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 doivent 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.

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

Les prestataires de services de paiement doivent 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 le soutiennent ainsi que les autres prestataires de services de paiement. Plus particulièrement, les prestataires de services de paiement doivent 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 doivent 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.

viii. *Impact en termes de réputation*

Les prestataires de services de paiement doivent 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 doivent 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 doivent déterminer si i) les utilisateurs de services de paiement et/ou d'autres prestataires de services de paiement se sont plaints des répercussions négatives de l'incident, ii) l'incident a affecté un processus visible lié aux services de paiement et est, par conséquent, susceptible de faire l'objet ou a déjà fait l'objet d'une couverture médiatique (en tenant compte non seulement des médias traditionnels, tels que les journaux, mais également des blogs, réseaux sociaux, etc.), iii) des obligations contractuelles n'ont pas été respectées, ou sont susceptibles de ne pas être respectées, entraînant la publication de demandes en justice contre le prestataire de services de paiement, iv) des obligations réglementaires n'ont pas été respectées, entraînant l'imposition de mesures de contrôle ou de sanctions qui ont été ou seront probablement rendues publiques, et v) un type d'incident similaire s'est déjà produit.

1.4. Les prestataires de services de paiement doivent évaluer un incident en déterminant, pour chaque critère individuel, si les seuils adéquats 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** durée de l'incident > 1 heure* **ou** > 500 000 EUR **et** durée de l'incident > 1 heure*	> 25 % du volume habituel des opérations du prestataire de services de paiement (en nombre d'opérations) **ou** > 15 000 000 EUR
Utilisateurs de services de paiement affectés	> 5 000 **et** durée de l'incident > 1 heure* **ou**	> 50 000 **ou**

	> 10 % des utilisateurs de services de paiement du prestataire de services de paiement **et** durée de l'incident > 1 heure*	> 25 % des utilisateurs de services de paiement du prestataire de services de paiement
Interruption du service	> 2 heures	Sans objet
Atteinte à la sécurité des réseaux ou des systèmes d'information	Oui	Sans objet
Impact économique	Sans objet	> Max (0,1 % des fonds propres de catégorie 1**, 200 000 EUR) **ou** > 5 000 000 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

* Le seuil relatif à la durée de l'incident au-delà d'une heure ne s'applique qu'aux incidents opérationnels qui affectent la capacité du prestataire de services de paiement à initier et/ou à traiter des opérations.

**Fonds propres de catégorie 1 tels que définis à l'article 25 du règlement (UE) nº 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) nº 648/2012.

1.5. Les prestataires de services de paiement doivent 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 doivent mener cette évaluation sur une base continue tout au long de l'incident, afin d'identifier tout changement de statut éventuel, ascendant (de non majeur à majeur) ou descendant (de majeur à non majeur). Tout déclassement de l'incident de majeur en non-majeur doit être notifié sans retard injustifié à l'autorité compétente, conformément aux exigences de l'orientation 2.21.

Orientation 2: Processus de notification

2.1. Les prestataires de services de paiement doivent recueillir toutes les informations pertinentes, rédiger une notification d'incident en complétant le modèle de l'annexe 1 et la soumettre à l'autorité compétente dans l'État membre d'origine. Les prestataires de services de paiement doivent compléter tous les champs du modèle en suivant les instructions fournies à l'annexe 1.

2.2. Les prestataires de services de paiement doivent utiliser le même modèle pour soumettre les rapports initial, intermédiaire et final relatifs à un même incident. Par conséquent, les prestataires de services de paiement doivent remplir un modèle unique de manière progressive et mettre à jour, le cas échéant, les informations fournies avec les précédents rapports.

2.3. Les prestataires de services de paiement doivent 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 doivent, à la demande de l'autorité compétente de l'État membre d'origine, fournir tout document supplémentaire complétant les informations soumises avec le modèle standardisé. Les prestataires de services de paiement doivent 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.

2.5. Toute information supplémentaire contenue dans les documents fournis par le prestataire de services de paiement à l'autorité compétente, soit à l'initiative du prestataire de services de paiement, soit à la demande de l'autorité compétente conformément à l'orientation 2.4, doit être mentionnée par le prestataire de services de paiement dans le modèle conformément à l'orientation 2.1.

2.6. Les prestataires de services de paiement doivent à tout moment préserver la confidentialité et l'intégrité des informations échangées et garantir leur authentification en bonne et due forme auprès de l'autorité compétente dans leur État membre d'origine.

Rapport initial

2.7. Les prestataires de services de paiement doivent soumettre un rapport initial à l'autorité compétente dans l'État membre d'origine dès qu'un incident opérationnel ou de sécurité a été classé comme majeur. Les autorités compétentes doivent accuser réception du rapport initial sans retard injustifié et attribuer un code de référence unique permettant d'identifier l'incident sans équivoque. Les prestataires de services de paiement doivent indiquer ce code de référence lorsqu'ils soumettent une mise à jour du rapport initial ou des rapports intermédiaire et final relatifs à un même incident, sauf si les rapports intermédiaire et final sont soumis conjointement avec le rapport initial.

2.8. Les prestataires de services de paiement doivent envoyer le rapport initial à l'autorité compétente dans un délai de quatre heures suivant la classification de l'incident opérationnel ou de sécurité comme incident «majeur». S'il est connu que les canaux de notification de l'autorité compétente ne sont pas disponibles ou opérationnels à ce moment-là, les

prestataires de services de paiement doivent envoyer le rapport initial dès que les canaux sont de nouveau disponibles/opérationnels.

2.9. Les prestataires de services de paiement doivent classer l'incident conformément aux orientations 1.1 et 1.4 dans les meilleurs délais dès que l'incident a été détecté – et en aucun cas plus de 24 heures après la détection de l'incident –, et sans retard injustifié après que les informations nécessaires à la classification de l'incident ont été mises à la disposition du prestataire de services de paiement. Si un délai supplémentaire est nécessaire pour classer l'incident, les prestataires de services de paiement doivent en expliquer les raisons dans le rapport initial soumis à l'autorité compétente.

2.10. Les prestataires de services de paiement doivent également soumettre un rapport initial à l'autorité compétente dans l'État membre d'origine lorsqu'un incident précédemment non majeur est reclassé en incident majeur. Dans ce cas particulier, les prestataires de services de paiement doivent envoyer le rapport initial 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.

2.11. Les prestataires de services de paiement doivent fournir dans leurs rapports initiaux (section A du modèle) des informations globales décrivant certaines caractéristiques fondamentales de l'incident et ses conséquences prévues sur la base des informations disponibles immédiatement après son classement en incident majeur. Les prestataires de services de paiement doivent avoir recours à des estimations lorsque des données réelles ne sont pas disponibles.

Rapport intermédiaire

2.12. Les prestataires de services de paiement doivent soumettre le rapport intermédiaire lorsque les activités habituelles ont été rétablies et que les affaires ont repris leur cours normal, en informant l'autorité compétente de cette situation. Les prestataires de services de paiement doivent 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 (délais de traitement, capacité, exigences de sécurité, etc.), et lorsque les mesures d'urgence ne sont plus en place. Le rapport intermédiaire doit comporter une description plus détaillée de l'incident et de ses conséquences (section B du modèle).

2.13. Si les activités habituelles n'ont pas encore été rétablies, les prestataires de services de paiement doivent soumettre un rapport intermédiaire à l'autorité compétente, dans un délai de trois jours ouvrables à compter de la date de soumission du rapport initial.

2.14. Les prestataires de services de paiement doivent mettre à jour les informations déjà fournies aux sections A et B du modèle lorsqu'ils prennent connaissance de changements significatifs

intervenus depuis la soumission du précédent rapport (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). Cela vaut notamment pour le cas où l'incident n'aurait pas été résolu dans un délai de trois jours ouvrables, ce qui obligerait les prestataires de services de paiement à soumettre un rapport intermédiaire supplémentaire. Dans tous les cas, les prestataires de services de paiement doivent soumettre un rapport intermédiaire supplémentaire à la demande de l'autorité compétente dans l'État membre d'origine.

2.15. Comme dans le cas des rapports initiaux, si des données effectives ne sont pas disponibles, les prestataires de services de paiement doivent utiliser des estimations.

2.16. Si l'activité est revenue à la normale avant qu'un délai de quatre heures se soit écoulé depuis le classement de l'incident en incident majeur, les prestataires de services de paiement doivent s'efforcer de soumettre simultanément le rapport initial et le rapport intermédiaire (à savoir, compléter les sections A et B du modèle) avant l'expiration du délai de quatre heures.

Rapport final

2.17. Les prestataires de services de paiement doivent soumettre un rapport final 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 que la cause profonde finale ait été identifiée ou non) et lorsque des chiffres réels sont disponibles pour remplacer les éventuelles estimations.

2.18. Les prestataires de services de paiement doivent remettre leur rapport final à l'autorité compétente dans un délai maximum de 20 jours ouvrables 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 ou que les causes profondes n'ont pas encore été identifiées) doivent contacter l'autorité compétente avant l'expiration de ce délai et fournir une justification adéquate du retard, ainsi qu'une nouvelle date estimée pour le rapport final.

2.19. Si les prestataires de services de paiement sont en mesure de fournir toutes les informations requises dans le rapport final (à savoir, la section C du modèle) dans le créneau de quatre heures suivant le classement de l'incident en incident majeur, ils doivent s'efforcer de soumettre simultanément les informations liées aux rapports initial, intermédiaire et final.

2.20. Les prestataires de services de paiement doivent inclure dans leur rapport final 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, ainsi qu'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 doivent également envoyer un rapport final 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 doivent envoyer le rapport final dès que cette situation est détectée et, en tout état de cause, avant la date limite pour la soumission du prochain rapport. Dans ce cas particulier, au lieu de compléter la section C du modèle, les prestataires de services de paiement doivent cocher la case «incident reclassé comme non majeur» et fournir une explication des 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 doivent 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; ou

   ii. dans les orientations de l'ABE sur les accords d'externalisation (EBA/GL/2019/02) concernant tous les prestataires de services de paiement.

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) doivent informer l'autorité compétente dans l'État membre d'origine, fournir 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. fournir la liste de tous les prestataires de services de paiement affectés par l'incident;

e. 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; s'assurer également qu'en cas de doute, 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;

f. s'assurer, lorsque le modèle comprend des champs où une réponse commune n'est pas possible (par exemple, les sections B2, B4 ou C3 du modèle), 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 les valeurs cumulatives telles qu'observées ou estimées pour les prestataires de services de paiement;

g. le tiers communique à tout moment au prestataire de services de paiement 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 du possible pour éviter toute 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 doivent 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 doivent 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 doivent 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 doivent satisfaire matériellement à 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 majeur opérationnel ou de sécurité conformément à l'article 96 de la DSP2 et aux présentes orientations. Les prestataires de services de paiement doivent également 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.

3.6. Les prestataires de services de paiement doivent veiller à ce que, dans le cas où un incident est occasionné par une perturbation des services fournis par un prestataire de services techniques (ou une infrastructure) qui affecte plusieurs PSP, la notification déléguée fasse référence aux données individuelles du prestataire de services de paiement (sauf en cas de notification consolidée).

Orientation 4: Politique opérationnelle et de sécurité

4.1. Les prestataires de services de paiement doivent s'assurer que leur politique générale opérationnelle et de sécurité 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 aux 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 communiquer à d'autres autorités nationales

Orientation 5: Évaluation de la pertinence de l'incident

5.1. Les autorités compétentes dans l'État membre d'origine doivent évaluer la pertinence d'un incident opérationnel ou de sécurité 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 doivent conduire cette évaluation sur une base continue tout au long de l'incident, de façon à 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 doivent fournir des informations au sujet d'incidents opérationnels ou de sécurité aux autorités nationales pertinentes identifiées en suivant l'application de l'orientation 5.1, au minimum, au moment de la réception du rapport initial (ou du rapport ayant conduit au partage des informations) et lorsqu'il leur est notifié que les affaires ont repris leur cours normal (à savoir, le rapport intermédiaire).

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

- date et heure de classement de l'incident en incident majeur;
- 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 prestataires de services de paiement et/ou infrastructures;
- description (le cas échéant) de la couverture médiatique;
- cause de l'incident.

6.3. Les autorités compétentes doivent 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 les autorités nationales pertinentes. Les autorités compétentes doivent néanmoins fournir aux 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 doivent à tout moment préserver la confidentialité et l'intégrité des informations stockées et échangées et garantir leur authentification en bonne et due forme auprès des autorités nationales pertinentes. Plus particulièrement, les autorités compétentes doivent 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 doivent 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 l'aide d'un fichier normalisé mis à disposition sur le site web de l'ABE.

Orientation 8: Communication

8.1. Les autorités compétentes doivent à tout moment préserver la confidentialité et l'intégrité des informations stockées et échangées et garantir leur authentification en bonne et due forme auprès de l'ABE et de la BCE. Plus particulièrement, les autorités compétentes doivent 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.

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

Annexe – Modèle de notification pour les prestataires de services de paiement

Rapport initial

Notification initiale	**dans les 4 heures suivant la classification de l'incident comme majeur.**			**Réinitialiser les sélections du menu**	
Date de la notification *(JJ/MM/AAAA)*		Heure *(HH:MM)*			
Code de référence de l'incident					

A - Notification initiale					
A 1 - INFORMATIONS GÉNÉRALES					
Type de notification					
Type de notification					
Prestataire de services de paiement (PSP) affecté					
Nom du PSP					
Numéro d'identification nationale du PSP					
Chef de groupe, le cas échéant					
Pays affecté(s) par l'incident	☐ AT ☐ BE ☐ BG ☐ CY ☐ CZ	☐ DE ☐ DK ☐ EE ☐ ES ☐ FI	☐ FR ☐ U ☐ GR ☐ HR ☐ HU	☐ IE ☐ IS ☐ IT ☐ LT ☐ LU	☐ LV ☐ MT ☐ NL ☐ NO ☐ PL	☐ PT ☐ RO ☐ SE ☐ SI ☐ SK
Personne de contact principale		Adresse électronique		Téléphone	
Personne de contact secondaire		Adresse électronique		Téléphone	
Entité notifiante (complétez cette section si l'entité notifiante n'est pas le PSP affecté en cas de notification déléguée)					
Nom de l'entité notifiante					
Numéro d'identification nationale					
Personne de contact principale		Adresse électronique		Téléphone	
Personne de contact secondaire		Adresse électronique		Téléphone	
A 2 - DÉTECTION et CLASSIFICATION DE L'INCIDENT					
Date et heure de détection de l'incident *(JJ/MM/AAAA HH:MM)*					
Date et heure de classification de l'incident *(JJ/MM/AAAA HH:MM)*					
L'incident a été détecté par		Si «Autres», veuillez préciser:			
Type d'incident					
Critères ayant déclenché la notification d'incident majeur	☐ Opérations affectées ☐ Utilisateurs de services de paiement affectés ☐ Interruption du service ☐ Atteinte à la sécurité des réseaux ou des systèmes d'information ☐ Impact économique ☐ Niveau élevé d'escalade interne ☐ Autres PSP ou infrastructures pertinentes potentiellement affectés ☐ Impact en termes de réputation				
Une description succincte et générale de l'incident					
Impact dans d'autres États membres de l'UE, le cas échéant					
Notification à d'autres autorités		Si «Oui», veuillez préciser:			
Motifs de la soumission tardive de la notification initiale					

Rapport intermédiaire

Notification d'incident majeur

Notification intermédiaire	au maximum 3 jours ouvrables à compter de la soumission de la notification initiale	Réinitialiser les sélections du
Date de la notification *(JJ/MM/AAAA)*		Heure *(HH:MM)*
Code de référence de l'incident		

B - Notification intermédiaire

B 1 - INFORMATIONS GÉNÉRALES

Description plus détaillée de l'incident:	
Quel est exactement le problème?	
Comment l'incident est-il survenu?	
Comment a-t-il évolué?	
Quelles sont les conséquences (en particulier pour les utilisateurs de services de paiement)?	
L'incident a-t-il été communiqué aux utilisateurs de services de paiement?	Si «Oui», veuillez préciser:
Était-il lié à un (des) incident(s) antérieur(s)?	Si «Oui», veuillez préciser:
D'autres prestataires de services/tiers ont-ils été affectés ou impliqués?	Si «Oui», veuillez préciser:
La gestion de crise a-t-elle été déclenchée (interne et/ou externe)?	Si «Oui», veuillez préciser:
Date et heure de classification de l'incident (si déjà établies) *(JJ/MM/AAAA HH:MM)*	
Date et heure auxquelles l'incident a été résolu ou devrait être résolu *(JJ/MM/AAAA HH:MM)*	
Domaines fonctionnels affectés	☐ Authentification/Autorisation ☐ Règlement direct ☐ Communication ☐ Règlement indirect ☐ Compensation ☐ Autres — Si «Autres», veuillez préciser:
Modifications apportées aux notifications précédentes	

B 2 - CLASSIFICATION DE L'INCIDENT/INFORMATIONS SUR L'INCIDENT

Opérations affectées [2]	Niveau d'impact Nombre d'opérations affectées En % du volume habituel des opérations Montant des opérations affectées en EUR Durée de l'incident (uniquement applicable aux incidents opérationnels) Remarques:
Utilisateurs de services de paiement affectés [3]	Niveau d'impact Nombre d'utilisateurs de services de paiement affectés En % du nombre total d'utilisateurs de services de paiement
Atteinte à la sécurité des réseaux ou des systèmes d'information	Indiquer comment les réseaux ou les systèmes d'information ont été affectés
Interruption du service	Interruption totale du service: — Jours: — Heures: — Minutes:
Impact économique	Niveau d'impact Coûts directs en EUR Coûts indirects en EUR
Niveau élevé de transmission à un niveau supérieur en interne	Décrivez le niveau de transmission à un niveau supérieur interne de l'incident, en indiquant s'il a déclenché ou est susceptible de déclencher un mode crise (ou équivalent) et, dans l'affirmative, veuillez décrire
Autres PSP ou infrastructures pertinentes potentiellement affectés	Décrivez la manière dont cet incident pourrait affecter d'autres PSP et/ou infrastructures
Impact en termes de réputation	Décrivez la manière dont l'incident pourrait affecter la réputation du PSP (par exemple, couverture médiatique, publication d'actions en justice ou violations de la législation...)

B 3 - DESCRIPTION DE L'INCIDENT

Type d'incident	
Cause de l'incident	☐ En cours d'enquête ☐ Action malveillante ☐ Défaillance des processus ☐ Défaillance des systèmes ☐ Erreurs humaines ☐ Événements externes ☐ Autres — Si «Autres», veuillez préciser:
L'incident vous a-t-il affecté directement ou indirectement par l'intermédiaire d'un prestataire de services?	Si «indirectement», veuillez indiquer le nom du prestataire de services:

B 4 - IMPACT DE L'INCIDENT

Impact global	☐ Intégrité ☐ Disponibilité ☐ Confidentialité ☐ Authenticité
Canaux commerciaux affectés	☐ Succursales ☐ Services bancaires par téléphone ☐ Point de vente ☐ Services bancaires en ligne ☐ Services bancaires mobiles ☐ Autres ☐ Commerce électronique ☐ Distributeurs automatiques de billets Si «Autres», veuillez préciser:
Services de paiement affectés	☐ Dépôt d'espèces sur un compte de paiement ☐ Virements ☐ Transmission de fonds ☐ Retrait d'espèces d'un compte de paiement ☐ Prélèvements automatiques ☐ Services ☐ Mesures requises pour exploiter un compte de paiement ☐ Paiements par carte ☐ Services d'information sur les comptes ☐ Acquisition d'instruments de paiement ☐ Émission d'instruments de paiement

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?	
Le plan de continuité des activités et/ou le plan de reprise après sinistre ont-ils été activés?	
Dans l'affirmative, quand? *(JJ/MM/AAAA HH:MM)*	
Dans l'affirmative, veuillez décrire	

Rapport final

Notification d'incident majeur

Veuillez sélectionner le type de notification:	au maximum 20 jours ouvrables à compter de la soumission de la notification intermédiaire	**Réinitialiser les sélections du menu déroulant**
Veuillez décrire: (applicable pour les incidents reclassés comme non majeurs)		
Date de la notification *(JJ/MM/AAAA)*		Heure *(HH:MM)*
Code de référence de l'incident		

C - Notification finale

Si aucune notification intermédiaire n'a été envoyée, veuillez également compléter la section B

C 1 - INFORMATIONS GÉNÉRALES

Mise à jour des informations tirées de la notification initiale et de la (des) notification(s) intermédiaire(s)	
Modifications apportées aux notifications précédentes	
Toute autre information pertinente	
Tous les contrôles initiaux sont-ils de nouveau en place?	
Si la réponse est «Non», précisez quels contrôles sont concernés ainsi que le délai supplémentaire nécessaire pour les rétablir	

C 2 - ANALYSE DES CAUSES PROFONDES ET SUIVI

Quelle était la cause profonde (si déjà connue)?	☐ Action malveillante ☐ Défaillance des ☐ Défaillance des ☐ Erreur humaine ☐ Événement externe ☐ Autres
Veuillez préciser:	☐ Code malveillant ☐ Collecte d'informations ☐ Intrusions ☐ Déni de Service/distribué (D/Dos) ☐ Actions internes délibérées ☐ Dommages physiques externes délibérés ☐ Sécurité du contenu de l'information ☐ Actions frauduleuses ☐ Autres ☐ Défaillance du suivi et du contrôle ☐ Problèmes de communication ☐ Opérations incorrectes ☐ Gestion inadéquate des changements ☐ Inadéquation des procédures internes et de la ☐ Problèmes de reprise après sinistre ☐ Autres ☐ Panne de matériel ☐ Défaillance de réseau ☐ Problèmes de base de données ☐ Défaillance de logiciels/d'applications ☐ Dommages ☐ Autres ☐ Involontaires ☐ Inaction ☐ Ressources insuffisantes ☐ Autres ☐ Défaillance d'un fournisseur/prestataire de services techniques ☐ Cas de force ☐ Autres Si «Autres», veuillez préciser:
Autres informations pertinentes sur la cause profonde	
Principales actions/mesures correctives prises ou prévues pour éviter que l'incident ne se reproduise à l'avenir, si déjà connues	

C 3 - INFORMATIONS SUPPLÉMENTAIRES

L'incident a-t-il été partagé avec d'autres PSP à titre d'information?	Dans l'affirmative, veuillez fournir des informations détaillées:
Une action en justice a-t-elle été intentée contre le PSP?	Dans l'affirmative, veuillez fournir des informations détaillées:
Évaluation de l'efficacité des mesures prises	Veuillez fournir des informations détaillées:

INSTRUCTIONS POUR REMPLIR LE MODÈLE

Les prestataires de services de paiement (PSP) doivent compléter la section pertinente du modèle, en fonction de la phase de notification dans laquelle ils se trouvent: la section A pour le rapport initial, la section B pour les rapports intermédiaires et la section C pour le rapport final. Les PSP doivent utiliser le même modèle pour soumettre les rapports initial, intermédiaire et final relatifs à un même incident. Tous les champs sont obligatoires, sauf disposition clairement contraire.

Titre

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

Rapport intermédiaire: elle contient une description plus détaillée de l'incident et de ses conséquences. Il s'agit d'une mise à jour du rapport initial (et, le cas échéant, d'un rapport intermédiaire précédent) concernant le même incident.

Rapport final: 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 et doit donc être reclassé.

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 doivent expliquer les raisons de ce reclassement.

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

Code de référence de l'incident (applicable aux rapports intermédiaire et final ainsi qu'aux mises à jour du rapport initial): le code de référence délivré par l'autorité compétente au moment du rapport initial pour identifier de manière unique l'incident. Chaque autorité compétente doit indiquer comme préfixe le code ISO à 2 chiffres[2] de son État membre respectif.

A - Rapport initial

A 1 - Informations générales

Type de notification:

individuelle: la notification concerne un seul PSP.

Consolidée: la notification concerne plusieurs PSP, au sein d'un même État membre, qui sont affectés par le même incident opérationnel ou de sécurité et qui utilisent la notification consolidée. Les champs sous «PSP affecté» doivent être laissés vierges (à l'exception du champ «Pays affecté(s) par l'incident») et une liste des PSP inclus dans la notification doit être fournie en complétant le tableau correspondant (Notification consolidée – Liste des PSP).

PSP affecté: il s'agit du 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 national du PSP: le numéro d'identification national unique utilisé par l'autorité compétente de l'État membre d'origine dans son registre national pour identifier sans équivoque le PSP.

Chef de groupe: dans le cas de groupes d'entités tels que définis à l'article 4, paragraphe 40, de la DSP2, veuillez indiquer le nom de l'entité mère.

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), quelle que soit la

[2] Veuillez vous référer aux codes pays alpha-2 selon ISO-3166 à l'adresse suivante: https://www.iso.org/iso-3166-country-codes.html

gravité de l'incident dans le ou les autres pays. 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, dans le cas où un prestataire de services 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. Dans le cas où un prestataire de services 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 doit être remplie dans le cas où un tiers s'acquitte des obligations de notification pour le compte du PSP affecté, le cas échéant.

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

Numéro d'identification nationale: le numéro d'identification national unique utilisé dans le pays où le tiers est situé pour identifier sans équivoque l'entité qui notifie l'incident. Si le tiers notifiant est un PSP, le numéro d'identification national doit être le numéro d'identification national unique du PSP utilisé par l'autorité compétente de l'État membre d'origine dans son registre national.

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 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 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 et classification de l'incident

Date et heure de détection de l'incident: la date et l'heure auxquelles l'incident a été identifié pour la première fois.

Date et heure de classification de l'incident: la date et l'heure auxquelles l'incident opérationnel ou de sécurité a été classé comme majeur.

Incident détecté par: indiquer si l'incident a été détecté par un utilisateur de services de paiement au sein du PSP (par exemple, fonction d'audit interne) ou par une autre partie externe (par exemple, prestataire de services). S'il ne s'agissait d'aucun de ceux-ci, veuillez fournir une explication dans le champ correspondant.

Type d'incident: indiquez si, à votre connaissance et si les informations sont disponibles, 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 et/ou l'authenticité 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 et/ou l'authenticité de services liés au paiement. Cela peut se produire notamment lorsque le PSP est confronté à une atteinte à la sécurité des réseaux ou des systèmes d'information.

Critères déclenchant la notification d'un incident majeur: veuillez indiquer quel(s) critère(s) a (ont) déclenché le rapport d'incident majeur. Plusieurs choix peuvent être sélectionnés parmi les critères: opérations affectées, utilisateurs de services de paiement affectés, durée de l'interruption de service, atteinte à la sécurité des réseaux ou des systèmes d'information, impact économique, niveau élevé d'escalade interne, autres PSP ou infrastructures pertinentes potentiellement affectés et/ou impact en termes de réputation.

Description succincte et générale de l'incident: veuillez expliquer brièvement les principaux points de l'incident, en précisant les causes possibles, les répercussions immédiates, etc.

Impact sur les autres États membres de l'UE, le cas échéant: veuillez expliquer brièvement l'impact que l'incident a eu dans un autre État membre de l'UE (par exemple sur les utilisateurs de services de paiement, les PSP et/ou les infrastructures de paiement). Si cela est possible dans les délais de notification applicables, veuillez fournir une traduction en anglais.

Notification à d'autres autorités: veuillez indiquer si l'incident a été ou sera notifié à d'autres autorités dans des cadres distincts de notification d'incidents (si cette information est connue au moment de la notification). Dans l'affirmative, veuillez préciser les autorités respectives.

Motifs de la soumission tardive du rapport initial: veuillez expliquer les raisons pour lesquelles vous avez eu besoin de plus de 24 heures pour classer l'incident.

B Rapport intermédiaire

B 1 – Informations générales

Description plus détaillée de l'incident: veuillez décrire les principales caractéristiques de l'incident, en précisant au moins les informations sur le problème spécifique et le contexte qui y est lié, comment l'incident a débuté et a évolué, ainsi que les conséquences, notamment pour les utilisateurs de services de paiement, etc. Veuillez également fournir des informations sur la communication avec les utilisateurs de services de paiement, le cas échéant.

Était-il lié à un (des) incident(s) antérieur(s)?: veuillez indiquer si l'incident est lié ou non à des incidents antérieurs (si cette information est disponible). Si l'incident est lié à des incidents antérieurs, veuillez préciser lesquels.

D'autres prestataires de services/tiers ont-ils été affectés ou impliqués?: veuillez indiquer si l'incident a ou non affecté ou impliqué d'autres prestataires de services/tiers (si cette information est disponible). Si l'incident a affecté ou impliqué d'autres prestataires de services/tiers, veuillez les énumérer et fournir davantage d'informations.

La gestion de crise (interne et/ou externe) a-t-elle été déclenchée?: veuillez indiquer si la gestion de crise (interne et/ou externe) a été déclenchée ou non. Si la gestion de crise a été déclenchée, veuillez fournir davantage d'informations.

Date et heure de début de l'incident: la date et l'heure auxquelles l'incident a débuté (si connues).

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.

Domaines fonctionnels affectés: indiquer la ou les étapes du processus de paiement qui ont été affectées par l'incident, telles que l'authentification/autorisation, la communication, la compensation, le règlement direct, le règlement indirect et autres.

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 des fonds.

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: 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 au moyen d'un transfert de fonds, lorsque cette action est réalisée par le PSP affecté lui-même.

Règlement indirect: l'exécution d'une opération ou d'un traitement dans le but de permettre aux participants de s'acquitter de leurs obligations par 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. Les informations complémentaires doivent être fournies dans le champ à texte libre.

Modifications apportées aux précédents rapports: veuillez indiquer les modifications apportées aux informations fournies avec les précédents rapports concernant un même incident (par exemple, le rapport initial ou, le cas échéant, un rapport intermédiaire).

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

Opérations affectées: Les PSP doivent 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 doivent fournir des valeurs concrètes pour ces variables, qui peuvent être des chiffres effectifs ou des estimations. En règle générale, les PSP doivent 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 ordonnées frauduleusement (que les fonds aient été récupérés ou non). En outre, les PSP doivent 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 doivent 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». Dans les cas où des opérations de paiement libellées dans des monnaies autres que l'euro sont affectées par l'incident, lors du calcul des seuils et de la déclaration de la valeur des opérations affectées, les PSP doivent convertir en euros le montant des opérations libellées dans une monnaie autre que l'euro en utilisant le taux de change de référence quotidien de la BCE en vigueur le jour précédant la soumission de la notification de l'incident.

Utilisateurs de services de paiement affectés: Les PSP doivent 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 doivent fournir des valeurs concrètes pour ces variables, qui peuvent être des chiffres effectifs ou des estimations. Les PSP doivent considérer comme des «utilisateurs de services de paiement affectés» tous les clients (nationaux ou étrangers, consommateurs ou entreprises) ayant un contrat avec le PSP affecté qui leur donne accès au service de paiement affecté, et qui ont subi ou subiront probablement les conséquences de l'incident. Les PSP doivent 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 doit 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 doit prendre en compte uniquement ses propres utilisateurs de services de paiement (le cas échéant), et les PSP bénéficiant de ces services opérationnels doivent également évaluer l'incident en rapport avec leurs propres utilisateurs de services de paiement. De plus, les PSP doivent 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.

Atteinte à la sécurité des réseaux ou des systèmes d'information: Les PSP doivent déterminer si une action malveillante a compromis la disponibilité, l'authenticité, l'intégrité ou la confidentialité des réseaux ou des systèmes d'information (y compris les données) liés à la fourniture de services de paiement.

Interruption du service: Les PSP doivent indiquer si le seuil a été ou sera probablement atteint par l'incident et le chiffre correspondant: interruption totale du service. Les PSP doivent fournir des valeurs concrètes pour cette variable, qui peuvent être des chiffres effectifs ou des estimations. Les PSP doivent 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 PSP doivent comptabiliser l'interruption de service à partir du moment où l'interruption se déclenche, et ils doivent 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 doivent exceptionnellement comptabiliser l'interruption de service à partir du moment où l'interruption est détectée.

Impact économique: Les PSP doivent indiquer si le seuil a été ou sera probablement atteint par l'incident et les chiffres correspondants: coûts directs et coûts indirects. Les PSP doivent fournir des valeurs concrètes pour ces variables, qui peuvent être des chiffres effectifs ou des estimations. Les PSP doivent prendre en compte les coûts qui peuvent être liés directement à l'incident et ceux qui sont indirectement liés à l'incident. Les PSP doivent, 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 remédiation, 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 doivent prendre en compte uniquement ceux qui sont déjà connus ou fortement susceptibles de se matérialiser. Dans les cas où les coûts sont libellés dans des monnaies autres que l'euro, lors du calcul du seuil et de la déclaration de la valeur de l'impact économique, les PSP doivent convertir en euros le montant des transactions libellées dans une monnaie autre que l'euro en utilisant le taux de change de référence quotidien de la BCE en vigueur le jour précédant la soumission de la notification de l'incident.

Coûts directs: les coûts (euros) directement causés par l'incident, y compris le coût pour corriger 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: les coûts (euros) indirectement causés par l'incident (par exemple, coûts de réparation/d'indemnisation des clients, coûts juridiques potentiels).

Niveau élevé d'escalade interne: Les PSP doivent déterminer si, en raison de l'impact sur les services liés au paiement, l'organe de direction, tel que défini par les orientations de l'ABE sur la gestion des risques liés aux TIC et à la sécurité, a été ou sera probablement informé de l'incident, conformément à l'orientation 60 d) des orientations de l'ABE sur la gestion des risques liés aux TIC et à la sécurité, 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 doivent 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.

Autres PSP ou infrastructures pertinentes potentiellement affectés: Les PSP doivent évaluer l'impact de l'incident sur le marché financier, entendu comme étant les infrastructures du marché financier et/ou les systèmes de paiement qui le soutiennent ainsi que les autres PSP. Plus particulièrement, les PSP doivent 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 doivent 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 doivent tenir compte du degré de visibilité que l'incident a, à leur connaissance, gagné ou gagnera probablement sur le marché. Plus particulièrement, les PSP doivent 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 doivent déterminer si i) les utilisateurs de services de paiement et/ou d'autres PSP se sont plaints des répercussions négatives de l'incident, ii) l'incident a affecté un processus visible lié aux services de paiement et est, par conséquent, susceptible de faire l'objet ou a déjà fait l'objet d'une couverture médiatique (en tenant compte non seulement des médias traditionnels, tels que les journaux, mais également des blogs, réseaux sociaux, etc., étant entendu, toutefois, que, dans ce contexte, la couverture médiatique ne se limite pas à quelques commentaires négatifs de suiveurs, mais qu'il doit y avoir un compte rendu valide ou un nombre important de commentaires négatifs/d'alertes), iii) des obligations contractuelles n'ont pas été respectées, ou sont susceptibles de ne pas être respectées, entraînant la publication de demandes en justice contre le prestataire de services de paiement, iv) des obligations réglementaires n'ont pas été respectées, entraînant l'imposition de mesures de contrôle ou de sanctions qui ont été ou seront probablement rendues publiques, et v) un type d'incident similaire s'est déjà produit.

B 3 – Description de l'incident

Type d'incident: opérationnel ou de sécurité. Des explications complémentaires sont fournies dans le champ correspondant du rapport initial.

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

En cours d'enquête: veuillez cocher cette case lorsque la cause n'est pas encore connue.

Action malveillante: actions ciblant délibérément le PSP. Il s'agit notamment des actions suivantes: code malveillant, collecte d'informations, intrusions, attaque par déni de service distribuée (D/DoS), actions internes délibérées, dommages physiques externes délibérés, sécurité du contenu des informations, actions frauduleuses et autres. Pour plus de précisions, veuillez vous reporter à la section C2 du présent modèle.

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, des réseaux, des infrastructures et des bases de données soutenant l'activité de paiement.

Erreurs humaines: 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).

Événements externes: la cause est associée à des événements échappant généralement au contrôle direct de l'entreprise (par exemple, catastrophes naturelles, défaillance d'un prestataire de services techniques).

Autre: la cause de l'incident ne fait pas partie des causes ci-dessus. Les informations complémentaires doivent 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?: veuillez indiquer si l'incident a ou non ciblé directement le PSP ou s'il l'affecte indirectement par l'intermédiaire d'un tiers (si ces informations sont disponibles). En cas d'impact indirect, veuillez fournir le nom du ou des prestataires de services.

B 4 – Impact de l'incident

Impact global: veuillez indiquer les dimensions qui ont été affectées par l'incident opérationnel ou de sécurité. Plusieurs choix peuvent être sélectionnés.

Intégrité: la propriété consistant à préserver l'exactitude et le caractère complet des actifs (y compris les données).

Disponibilité: la propriété selon laquelle les services liés au paiement sont pleinement accessibles et utilisables par des utilisateurs de services de paiement, selon des niveaux acceptables prédéfinis.

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.

Canaux commerciaux affectés: 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 doivent 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.

Commerce électronique: l'opération de paiement est initiée dans un point de vente virtuel (par exemple, pour les paiements initiés via l'internet au moyen de virements, de cartes de paiement ou de transferts d'argent électronique entre comptes de monnaie électronique).

Autre: le canal commercial affecté ne fait pas partie des catégories ci-dessus. Les informations complémentaires doivent 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 PSP du bénéficiaire ou au propre PSP 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 du bénéficiaire et mis à la disposition de ce dernier.

Services d'initiation de paiement: un service 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 détenu(s) par l'utilisateur de services de paiement chez un autre PSP ou plusieurs PSP.

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 de reprise après sinistre ont-ils été activés?: veuillez indiquer si c'est le cas 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).

C – Rapport final

C 1 – Informations générales

Mise à jour des informations à partir du rapport initial et du (des) rapport(s) intermédiaire(s) (résumé): veuillez fournir des informations complémentaires sur l'incident, y compris les modifications spécifiques apportées aux informations fournies avec le rapport intermédiaire. Veuillez également ajouter toute autre information pertinente.

Tous les contrôles d'origine sont-ils de nouveau en place?: veuillez indiquer si le PSP a dû ou non annuler ou affaiblir certains contrôles au cours de l'incident. Dans l'affirmative, veuillez indiquer si tous les contrôles sont de nouveau en place, et si ce n'est pas le cas, précisez dans le champ à texte libre les contrôles qui n'ont pas été rétablis et le délai supplémentaire nécessaire pour les rétablir.

C 2 – Analyse des causes profondes et suivi

Quelle était la cause profonde, si elle est déjà connue?: veuillez indiquer quelle est la cause profonde de l'incident ou, si elle n'est pas encore connue, celle qui est la plus probable. Plusieurs choix peuvent être sélectionnés. (Veuillez noter que la cause profonde doit être distinguée de l'impact de l'incident.)

Action malveillante: actions externes ou internes ciblant délibérément le PSP. Ces actions se divisent en plusieurs catégories:

Code malveillant: par exemple un virus, un ver, un cheval de Troie, un logiciel espion.

Collecte d'informations: par exemple, le «scanning», le «sniffing», l'ingénierie sociale.

Intrusions: par exemple, la compromission d'un compte privilégié, la compromission d'un compte non privilégié, la compromission d'une application, les bots.

Attaque par déni de service distribuée (D/DoS): une tentative ayant pour but de rendre un service en ligne indisponible en l'inondant d'un trafic provenant de sources multiples.

Actions internes délibérées: par exemple, sabotage, vol.

Dommages physiques externes délibérés: par exemple, sabotage, attaque physique des locaux/centres de données.

Sécurité du contenu de l'information: accès non autorisé aux informations, modification non autorisée des informations.

Actions frauduleuses: utilisation non autorisée des ressources, droits d'auteur, «masquerade», hameçonnage.

Autres (veuillez préciser): la cause de l'incident ne fait pas partie des causes ci-dessus. Les informations complémentaires doivent être fournies dans le champ à texte libre.

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). Ces défaillances se divisent en plusieurs catégories:

Défaillance du suivi et du contrôle: par exemple, en ce qui concerne les opérations de fonctionnement, les dates d'expiration des certificats, les dates d'expiration des licences, les dates d'expiration des correctifs, les contre-valeurs maximales définies, les niveaux de remplissage des bases de données, la gestion des droits des utilisateurs, le principe du double contrôle.

Problèmes de communication: par exemple, entre les opérateurs du marché ou au sein de l'organisation.

Opérations incorrectes: par exemple, non-échange de certificats, cache complet.

Gestion inadéquate des changements: par exemple, erreurs de configuration non identifiées, déploiement avec mises à jour, problèmes de maintenance, erreurs inattendues.

Inadéquation des procédures internes et de la documentation: par exemple, manque de transparence concernant les fonctionnalités, les processus et la survenue de dysfonctionnements, absence de documentation.

Problèmes de reprise après sinistre: par exemple, gestion des sinistres, redondance inadéquate.

Autres (veuillez préciser): la cause de l'incident ne fait pas partie des causes ci-dessus. Les informations complémentaires doivent être fournies dans le champ à texte libre.

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, des réseaux, des infrastructures et des bases de données soutenant l'activité de paiement. Ces défaillances se divisent en plusieurs catégories:

Panne de matériel: défaillance des équipements technologiques physiques qui exécutent les processus et/ou stockent les données dont les PSP ont besoin pour mener à bien leur activité liée au paiement (par exemple, défaillance des disques durs, des centres de données ou d'autres infrastructures).

Défaillance de réseau: défaillance des réseaux de télécommunications (publics ou privés) qui permettent l'échange de données et d'informations (par exemple via l'internet) pendant le processus de paiement.

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

Défaillance de logiciels/d'applications: défaillances des programmes, des systèmes d'exploitation, etc., qui soutiennent la fourniture des services de paiement par le PSP (par exemple, dysfonctionnements, fonctions inconnues).

Dommages physiques: par exemple, dommages involontaires causés par des conditions inadéquates, travaux de construction.

Autre (veuillez préciser): la cause de l'incident ne fait pas partie des causes ci-dessus. Les informations complémentaires doivent être fournies dans le champ à texte libre.

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). Ces erreurs se répartissent dans les catégories suivantes:

Involontaires: par exemple, erreurs, omissions, manque d'expérience et de connaissances.

Inaction: par exemple, en raison d'un manque de compétences, de connaissances, d'expérience ou de sensibilisation.

Ressources insuffisantes: par exemple, manque de ressources humaines, disponibilité du personnel.

Autre (veuillez préciser): la cause de l'incident ne fait pas partie des causes ci-dessus. Les informations complémentaires doivent être fournies dans le champ à texte libre.

Événement externe: la cause est associée à des événements qui échappent généralement au contrôle de l'organisation. Ces erreurs se répartissent dans les catégories suivantes:

Défaillance d'un fournisseur/prestataire de services techniques: par exemple, coupure d'électricité, panne internet, problèmes juridiques, problèmes commerciaux, dépendances des services.

Force majeure: par exemple, panne d'électricité, incendie, causes naturelles telles que tremblements de terre, inondations, fortes précipitations ou rafales de vent.

Autre (veuillez préciser): la cause de l'incident ne fait pas partie des causes ci-dessus. Les informations complémentaires doivent être fournies dans le champ à texte libre.

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

Autres informations pertinentes sur la cause profonde: veuillez fournir des précisions supplémentaires sur la cause profonde, y compris les conclusions préliminaires tirées de l'analyse des causes profondes.

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.

Évaluation de l'efficacité des mesures prises: veuillez inclure, le cas échéant, une autoévaluation de l'efficacité des mesures prises au cours de l'incident, y compris les enseignements tirés de l'incident.