Paris, le 20/12/2021

Division des services financiers

Dispositif technique relatif à la notification des incidents opérationnels et de sécurité majeurs au titre de l'article 96(3) de la 2e Directive européenne sur les Services de Paiements (DSP2)

Les orientations de l'Autorité bancaire européenne (ABE) prises en application de l'article 96(3) de la 2e directive européenne sur les services de paiement ont été publiées dans leur première version le 27 juillet 2017 avec une entrée en application fixée au 13 janvier 2018 (EBA/GL/2017/09). L'obligation de notification des incidents opérations ou de sécurité majeur a été transposée dans la loi française à l'article L.521-10 (étendu à la Polynésie française en vertu de l'article L.755-8, à la Nouvelle-Calédonie en vertu de l'article L.745-8 et dans les îles Wallis-et-Futuna en vertu de l'article L.765-8) qui dispose que les incidents opérationnels majeurs sont notifiés par les prestataires de services de paiement (PSP) à l'Autorité de contrôle prudentiel et de résolution (ACPR) et que les incidents de sécurité majeurs sont notifiés à l'Institut d'émission d'Outre-Mer (IEOM) s'agissant des établissements implantés dans les Collectivités du Pacifique. Toutefois, la notification se fait par le biais d'une interface commune à l'IEOM, la BDF et l'ACPR.

L'objet de cette note est (i) de présenter les changements apportés par la révision publiée en 2021 des orientations de l'ABE sur la notification des incidents majeurs et (ii) de rappeler la procédure et les modalités techniques à suivre pour assurer cette notification aux autorités.

1) Orientations révisées de l'Autorité bancaire européenne (ABE) relative à la notification d'incidents opérationnels ou de sécurité majeurs au titre de la DSP2

L'Autorité Bancaire Européenne (ABE) a publié le 10 juin 2021 une version révisée des orientations relatives à la déclaration d'incidents majeurs (EBA/GL/2021/03). En effet, conformément à l'article 96(4), ces orientations doivent être examinées à intervalles réguliers et en tout état de cause au moins tous les deux ans, dans le cadre de l'amélioration continue du processus de supervision.

Cette nouvelle version entre en application le **1er janvier 2022**. Celle-ci vise en particulier à :

- Optimiser et simplifier les modèles de rapports afin d'améliorer la qualité des déclarations reçues et de recevoir des données plus harmonisées ;
- Affiner les critères de façon à mieux informer les autorités des incidents de sécurité qui, sur la base des critères actuels ne seraient pourtant pas considérés comme majeurs, alors que l'expérience montre qu'ils sont importants ;

- Réduire le nombre d'incidents opérationnels signalés, qui sont actuellement classés comme majeurs mais qui ne sont pas nécessairement significatifs en réalité.

2) Synthèse des changements apportés par rapport à la première version publiée en 2017

La mise à jour des orientations de l'EBA sur les incidents majeurs porte essentiellement sur :

- La modification et l'ajout de critères et de seuils de façon pour les autorités à être destinataires de plus d'incidents de sécurité et de moins d'incidents opérationnels peu significatifs. Pour ce faire, il est introduit le critère « *Atteinte à la sécurité des réseaux ou des systèmes d'information* » de façon à être notifié des incidents majeurs liés aux actions malveillantes subies par les PSP. Ces actions malveillantes doivent avoir un impact négatif sur la sécurité des réseaux ou des systèmes d'information liés à la fourniture de services de paiement. Dans le même temps, les PSP ne doivent notifier que les incidents opérationnels d'une durée supérieure à une heure.

- L'amélioration du dispositif de notification (procédures de signalement, modèle de rapport…). Le modèle de rapport a été revu afin de simplifier la saisie par les PSP, améliorer la qualité des rapports reçus et recevoir des données plus harmonisées.

- L'attribution d'une référence unique par l'autorité de surveillance, afin de permettre l'identification de chaque incident sans équivoque et d'assurer sa traçabilité tout au long de son cycle de vie. L'IEOM et la Banque de France recommandent de mettre en place la convention de nommage suivante : **FR_CIB_AAAA_X** :

    - **FR** : pour préciser que le PSP concerné est autorisé et supervisé en France ;
    - **CIB** : le code interbancaire de l'établissement qui déclare l'incident ;
    - **AAAA** : l'année de la détection de l'incident ;
    - **X** : un numéro incrémental (1,2,3 etc.).

Pour un même incident, le PSP doit utiliser la même référence pour les notifications initiale, intermédiaire et finale. Les prestataires de services de paiement doivent donc utiliser **un fichier unique doté d'une référence unique**, qu'ils remplissent et communiquent de manière progressive au fur et à mesure des trois notifications.

3) Tableau comparatif des critères de qualification des incidents majeurs

Le tableau ci-dessous compare les critères de classification utilisés dans les orientations publiées en juin 2021 par rapport à celles de 2017.

a. Critères de qualification modifiés

	Version applicable jusqu'au 31/12 /21		Version applicable au 01/01/2022	
Critères	**Niveau d'impact inférieur** *(trois critères ou plus)*	**Niveau d'impact supérieur** *(un ou plusieurs critères)*	**Niveau d'impact inférieur** *(trois critères ou plus)*	**Niveau d'impact supérieur** *(un ou plusieurs critères)*
Opérations affectées	> 10 % du volume habituel des opérations du prestataire de services de paiement (en nombre d'opérations) ***et*** > 100 000 EUR	> 25 % du volume habituel des opérations du prestataire de services de paiement (en nombre d'opérations) ***ou*** > 5 millions EUR	> 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*** > 10 % des utilisateurs de services de paiement du prestataire de services de paiement	> 50 000 ***ou*** > 25 % des utilisateurs de services de paiement du prestataire de services de paiement	> 5 000 ***et*** durée de l'incident > 1 heure* ***ou*** > 10 % des utilisateurs de services de paiement du prestataire de services de paiement ***et*** durée de l'incident > 1 heure*	> 50 000 ***ou*** > 25 % des utilisateurs de services de paiement du prestataire de services de paiement
Atteinte à la sécurité des réseaux ou des systèmes d'information	***Critère inexistant***	***Critère inexistant***	**Oui (nouveau critère)**	**Sans objet**

b. Critères de qualification inchangés

	Version applicable jusqu'au 31/12 /21		Version applicable au 01/01/2022	
Critères	**Niveau d'impact inférieur** *(trois critères ou plus)*	**Niveau d'impact supérieur** *(un ou plusieurs critères)*	**Niveau d'impact inférieur** *(trois critères ou plus)*	**Niveau d'impact supérieur** *(un ou plusieurs critères)*
Interruption du service	> 2 heures	**Sans objet**	> 2 heures	**Sans objet**
Impact économique	***Sans objet***	> Max (0,1 % des fonds propres de catégorie 1**, 200 000 EUR) ***ou*** > 5 000 000 EUR	***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	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***	Oui	***Sans objet***
Impact en termes de réputation	Oui	***Sans objet***	Oui	***Sans objet***

4) Structure et cycle de vie des rapports d'incidents

Le modèle de rapport d'incident est accessible sous le lien suivant :

https://www.banque-france.fr/sites/default/files/media/2021/10/01/00_rapport-d-incident-majeur-modele.zip

Les rapports d'incidents sont constitués d'un ensemble de champs structurés, répartis en trois grandes sections A, B et C qui correspondent aux différentes étapes du cycle de vie de l'incident.

- **Rapport initial** : il doit être transmis par le PSP dans un délai de 4 heures suivant la classification de l'incident opérationnel ou de sécurité comme incident majeur, et contient au minimum les informations décrites dans la section A.

- **Rapport(s) intermédiaire(s)** : le premier rapport intermédiaire doit être remis au maximum dans les 3 jours suivant la transmission du rapport initial. Un nouveau rapport peut être soumis autant de fois que nécessaire suivant l'évolution de l'incident ou sur demande de l'autorité. Il contient au minimum les informations décrites dans la section B. De façon exceptionnel, si un incident est résolu dans les 4 heures suivant la période de détection, les données du rapport intermédiaire peuvent être remises en même temps que le rapport initial.

- **Rapport final :** il doit être remis au maximum dans un délai de 20 jours ouvrables à compter de la transmission de la notification intermédiaire. Il contient au minimum les informations décrites dans la section C. Si un incident est résolu dans les 4 heures suivant la période de détection, un rapport unique contenant toutes les informations des sections A, B et C peut être soumis.

Enfin, à condition de respecter les conditions posées par les Orientations de l'ABE – cf. l'orientation n°3 - et d'en informer préalablement l'IEOM et l'ACPR, la déclaration des incidents majeurs peut être déléguée à un sous-traitant, qui émet alors un rapport consolidé pour le compte des différents PSPs affectés. Dans ce cas de figure, la structure du rapport demeure la même, avec l'ajout d'un tableau complémentaire récapitulant la liste des PSPs impactés.

> ***Important :*** *Ces trois rapports sont communiqués via un fichier unique doté d'une référence unique, que les PSPs remplissent et communiquent au fur et à mesure. Chacune de ces notifications peut être accompagnée, si le PSP le juge opportun, de documents complémentaires transmis sous format libre (PDF, Word, Excel…).*

5) Plateforme SHAREBOX de notification des incidents majeurs

Les PSP disposant d'un délai réduit (au plus 4 heures) pour remettre le rapport initial à la suite de la détection d'un incident : les rapports peuvent être soumis **au fil de l'eau, 24h/24 et 7j/7, toute l'année**.

À cet effet, l'IEOM, la BDF et l'ACPR mettent à disposition des déclarants une plateforme commune de type SHAREBOX de notification des incidents qui assure la confidentialité, l'authenticité et l'intégrité des informations échangées.

Les demandes d'accréditation à la plateforme ou de documentation doivent être adressés par courriel à : 2323-NOTIFICATIONS-UT@banque-france.fr, copie IEOM-Paris-SEF-Surveillance@iedom-ieom.fr, en précisant dans le corps du message les informations suivantes :

- Raison sociale de l'établissement, numéro de CIB, adresse postale ;
- Fonction et coordonnées des représentants de l'établissement en charge de la déclaration des incidents majeurs (adresse mail, numéro de téléphone fixe ou mobile).

Le guide utilisateur de cette interface est accessible sous le lien suivant :

https://www.banque-france.fr/sites/default/files/media/2018/03/08/notif_3_-_guide_utilisateur.pdf

Note : l'activation des liens proposés peut nécessiter de coller directement l'adresse dans votre navigateur