Annexe - Référentiel de sécurité du chèque

Identification et notification des incidents graves sur le système de paiement par chèque

Le Référentiel de Sécurité du Chèque (RSC) et le questionnaire d'évaluation associé prévoit pour chaque objectif de sécurité que l'établissement adapte son niveau de cotation en fonction de certains critères d'appréciation. Un de ces critères, qui est applicable à tous les objectifs de sécurité, est lié aux incidents graves et à l'augmentation significative de la fraude.

Le RSC définit l'incident grave mais n'avait jusqu'ici pas défini de critères ni d'indicateurs applicables permettant la qualification des incidents graves, à l'instar des orientations de l'Autorité Bancaire Européenne[1] (ABE), qui définissent les critères permettant de qualifier comme « majeur » les incidents opérationnels ou de sécurité affectant les services de paiement encadrés par la 2e directive européenne sur les services de paiement (Directive UE n°2015/2366, dite DSP2). L'identification des incidents graves revenait donc à chaque établissement selon sa propre méthode d'évaluation, ce qui ne garantissait pas la convergence des approches sur ces critères d'appréciation.

La Banque de France a souhaité, lors de la révision du RSC conduite en 2022, définir des critères communs pour l'identification des incidents graves par les établissements assujettis ainsi que les procédures que les établissements doivent appliquer pour notifier ces incidents graves à la Banque de France, comme le prévoit l'objectif de sécurité 4 – « *Gestion des incidents et reporting* ». Ces critères communs ont été repris par l'IEOM à l'identique pour l'identification des incidents graves qui doivent lui être notifiés.

[1] EBA/GL/2021/03 du 10 juin 2021 Orientations révisées sur la notification des incidents majeurs en vertu de la DSP2

1) Définitions des incidents graves dans le RSC

Un incident grave est considéré dans le RSC comme une « *incapacité à rendre* (sur l'un des processus liés au système de paiement par chèque*) le service attendu, qui touche un nombre important d'opérations, en volume et en valeur, et qui a des conséquences juridiques pour l'établissement et/ou les autres acteurs du SPC, en termes juridiques, d'image, opérationnels, financiers et est susceptible de générer des retards, des coûts, des pertes* ».

Il ne s'agit donc pas des incidents d'exploitation courants affectant les processus liés au système de paiement par chèque.

2) Critères de qualification en tant qu'incident grave

2.1 Les établissements doivent qualifier comme graves les incidents opérationnels ou de sécurité qui remplissent

- un ou plusieurs critères au « niveau d'impact supérieur », ou
- trois critères ou plus au « niveau d'impact inférieur »

comme le prévoit le tableau du point 2.4.

2.2 Si un incident qualifié comme grave en vertu du RSC est également qualifié comme incident majeur en vertu de la DSP2, l'établissement est alors autorisé à ne faire qu'une seule notification d'incident majeur à l'IEOM. Il peut par exemple s'agir d'incidents affectant les canaux de banque à distance, si ceux-ci participent aussi aux processus de commande de chéquiers, de remises de chèque ou de mises en opposition.

2.3 Les établissements doivent évaluer un incident opérationnel ou de sécurité par rapport aux critères suivants :

2.3.1 Opérations affectées

Les établissements doivent déterminer le montant total des opérations de paiement par chèques affectées par l'incident, ainsi que le nombre de paiements par chèque compromis en pourcentage du volume habituel quotidien des opérations de paiement par chèque compris, non traité dans les deux jours ouvrés suivant le début de l'incident.

Le volume moyen quotidien est calculé comme étant le volume annuel de chèques traités par un établissement en tant qu'établissement tiré ou établissement remettant sur l'année n-1, divisé par le nombre de jours ouvrés dans l'année n (par exemple en 2022 : 253 jours ouvrés pour une entreprise ouverte du lundi au vendredi).

L'établissement appréhende ce critère à la fois comme établissement destinataire (ou le cas échéant établissement tiré) et comme établissement remettant (ou le cas échéant établissement du remettant). Cela s'applique donc aux incidents opérationnels qui affectent la capacité de l'établissement à traiter les remises de chèque ou respectivement à traiter les chèques présentés au paiement. Par exemple, un incident sera qualifié comme grave s'il affecte un volume de chèque remis à l'encaissement supérieur à 50% du volume quotidien des opérations de remise de chèque et que cet incident n'est pas résolu ou ne sera pas résolu dans les deux jours ouvrés suivant le début de l'incident.

2.3.2 Nombre de chèques perdus ou volés

Les établissements doivent déterminer le nombre de chèques perdus ou volés concernés par l'incident, qu'il s'agisse de formules, de chèques émis ou de vignettes. Seules les pertes et les vols intervenant dans les processus placés sous la responsabilité de l'établissement sont concernés, excluant donc les pertes et les vols intervenant dans le circuit postal ou chez les utilisateurs.

2.3.3 Atteinte à la sécurité des réseaux, des systèmes d'information ou des locaux dédiés au traitement du chèque

Les établissements doivent déterminer si une action malveillante a compromis la sécurité des réseaux, des systèmes d'information ou des locaux liés aux activités du système de paiement par chèque de l'établissement. Cela couvre les actions malveillantes touchant les prestataires, auprès desquels l'établissement délègue certains traitements liés aux systèmes de paiement par chèque.

2.3.4 Interruption d'un service lié au système de paiement par chèque

Les établissements doivent déterminer la durée pendant laquelle certains services liés au système de paiement par chèque sont indisponibles. Il s'agit de (i) la plateforme de mise en opposition des chèques, (ii) des services de remise à l'encaissement de chèques et leur traitement et (iii) des services liés à la fabrication et à la remise des formules.

Pour la plateforme de mise en opposition des chèques, il s'agit de tout incident affectant un canal utilisé pour la mise en opposition (canal téléphonique, banque en ligne, application bancaire) ainsi que tout outil utilisé par l'établissement bancaire pour déclarer ces oppositions au Fichier national des chèques irréguliers (FNCI) tenu par la Banque de France.

2.3.5 Impact financier

Les établissements 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 de l'établissement (à savoir, par rapport aux fonds propres de catégorie 1 du prestataire de services de paiement). Les fonds propres de catégorie 1 sont 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.

2.3.6 Niveau élevé d'escalade interne

Les établissements devraient déterminer si cet incident a été ou sera probablement notifié à leurs cadres supérieurs.

2.3.7 Autres acteurs du SPC ou infrastructures pertinentes potentiellement affectés

Les établissements devraient déterminer les implications systémiques que l'incident est susceptible d'entraîner, à savoir ses retombées potentielles, non seulement sur l'établissement initialement affecté, mais également sur les autres acteurs du SPC et établissements financiers.

2.3.8 Impact en termes de réputation

Les établissements devraient déterminer dans quelle mesure l'incident peut porter atteinte à la confiance accordée par les utilisateurs à l'établissement lui-même et plus généralement au système de paiement par chèque.

2.4 Les établissements doivent évaluer un incident en déterminant, pour chaque critère individuel, si les seuils adéquats du tableau ci-dessous sont ou seront probablement atteints avant la résolution de l'incident.

Critères	Niveau d'impact inférieur	Niveau d'impact supérieur
Opérations de paiement par chèque affectées (en tant qu'établissement tiré ou en tant qu'établissement remettant)	> 20 % du volume moyen quotidien des opérations de l'établissement **et** durée de l'incident > 2 jours ouvrés	> 50 % du volume moyen quotidien des opérations de l'établissement (en nombre d'opérations de paiement par chèque) **et** durée de l'incident > 2 jours ouvrés
Nombre de chèques perdus ou volés (formules, chèques, ou vignettes), dans le circuit sous la responsabilité de l'établissement (hors les vols/pertes intervenus dans le circuit postal ou chez le client)	> 2 000	> 20 000
Interruption d'un service lié au chèque	> 2 heures pour la plateforme de mise en opposition des chèques > 2 jours ouvrés pour les services de remise à l'encaissement de chèques et leur traitement > 10 jours ouvrés pour les services liés à la remise des formules	*Sans objet*
Atteinte à la sécurité des réseaux, des systèmes d'information ou des locaux dédiés au traitement du chèque	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 par chèque ou infrastructures pertinentes potentiellement affectés	Oui	*Sans objet*

Impact en termes de réputation	Oui	*Sans objet*

2.5 Les établissements 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).

2.6 Les établissements 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 grave à grave) ou descendant (de grave à non grave). Tout déclassement de l'incident de grave en non grave doit également être notifié sans retard injustifié à l'IEOM.

2.7 Ces critères communs doivent au minimum être pris en compte et déclinés dans les procédures de l'établissement, mais celui-ci peut les compléter ou les préciser dans sa procédure interne de qualification des incidents affectant les procédures liées au système de paiement par chèque.

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

Le modèle de rapport d'incident est téléchargeable sur l'espace Sharebox dédié aux déclarations d'incidents majeurs:

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 l'établissement dans un délai de 4 heures suivant la classification de l'incident comme incident grave, 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'IEOM. 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 par l'objectif 4 du RSC, la déclaration des incidents graves peut être déléguée à un sous-traitant, qui émet alors un rapport consolidé pour le compte des différents établissements affectés. Dans ce cas de figure, la structure du rapport demeure la même, avec l'ajout d'un tableau complémentaire récapitulant la liste des établissements impactés.

Ces trois rapports sont communiqués via un fichier unique doté d'une référence unique, que les établissements remplissent et communiquent au fur et à mesure. Chacune de ces notifications peut être accompagnée, si l'établissement le juge opportun, de documents complémentaires transmis sous format libre (PDF, Word, Excel…). Pour **la référence unique**, l'IEOM recommande la convention de nommage suivante : **CHQ_CIB_AAAA_X** :

- CHQ : pour préciser que l'incident affecte le système de paiement par chèque ;
- CIB : le code interbancaire de l'établissement qui déclare l'incident (ou la raison sociale du prestataire si c'est le prestataire qui effectue la notification
- AAAA : l'année de la détection de l'incident
- X : un numéro incrémental (1,2,3 etc.).

4) Plateforme SHAREBOX de notification des incidents graves

Les établissements 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 met à disposition des déclarants une plateforme commune - développée par la Banque de France - 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 mémo-utilisateur de cet espace confidentiel peut être transmis sur simple demande à IEOM-Paris-SEF-Surveillance@iedom-ieom.fr