FAQ – Annexe au rapport annuel de contrôle interne portant sur la sécurité des moyens de paiement scripturaux

Cette FAQ est destinée à aider les établissements assujettis dans la rédaction du nouveau modèle d'annexe relative à la sécurité des moyens de paiement scripturaux du rapport de contrôle interne qui entre en vigueur à compter de l'exercice 2017.

Questions / Réponses

1. **Comment comprendre la notion de canal d'initiation pour la description de l'offre de produits et services de chaque moyen de paiement ainsi que pour la partie relative à l'analyse des risques de fraude ?**

   Selon les différents moyens de paiement, la notion de canal d'initiation correspond :
   - pour la carte, au canal d'utilisation de la carte : paiement point de vente, retrait, paiement à distance, sans contact, enrôlement dans des *wallets* internet (Paylib, LyfPay,…) ou des solutions de paiement mobile (Apple Pay, Paylib,…);
   - pour le virement, au canal de réception de l'ordre de virement : guichet, espace de banque en ligne, solution de télétransmission… ;
   - pour le prélèvement, au canal de réception des ordres de prélèvement ;
   - pour le chèque, au canal de remise du chèque : courrier, automate…

2. **Quel est le niveau de granularité attendu pour la présentation de l'organisation opérationnelle de l'activité de chaque moyen de paiement ?**

   Cette partie doit indiquer, de façon synthétique, les différents acteurs impliqués dans les chaines de traitement dans leur ensemble, depuis l'émission ou la réception du moyen de paiement jusqu'à sa remise aux systèmes d'échange ou son imputation en compte. Il convient donc de préciser les activités directement traitées par le groupe (et les entités / directions concernées le cas échéant) et les traitements externalisés auprès de prestataires externes. L'insertion d'un schéma d'organisation explicatif est possible pour limiter le cas échéant la quantité d'information à fournir dans le tableau.

3. **Concernant la carte, il est demandé de décrire les mesures de couverture pour chacune des typologies de fraude. Or, lorsque l'établissement se place en qualité d'acquéreur il n'a pas connaissance des typologies de fraude des transactions fraudées. Quelle est donc l'information attendue ?**

   Il convient de décrire succinctement le dispositif en place (et envisagé à court terme) pour lutter contre les différentes typologies de fraude carte telles qu'elles sont retenues pour la collecte « Recensement de la fraude sur les moyens de paiement scripturaux » faite par la Banque de France ; cet exercice ne nécessite donc pas de connaitre les statistiques de fraude par typologie.

À titre d'exemple, en tant qu'établissement acquéreur ces mesures de couverture peuvent être :

- pour le vol/perte de carte : l'utilisation de la liste d'opposition…
- pour la carte falsifiée ou contrefaite : le dispositif d'autorisation *off-line* ou *on-line*…
- pour le numéro de carte usurpé : le recours au protocole 3D-Secure pour demander une authentification par la banque émettrice de la carte…

Les établissements ont toute latitude pour utiliser la rubrique « autres typologies de fraude » pour y renseigner des mesures de couverture visant d'autres catégories de fraude.

4. Concernant la partie relative à l'évaluation de la conformité aux recommandations d'organismes externes en matière de sécurité des moyens de paiement, comment doivent répondre les établissements qui externalisent leurs activités de paiement ?

Lorsque l'établissement externalise son activité de paiement auprès d'un prestataire lui-même assujetti à l'élaboration de l'annexe relative à la sécurité des moyens de paiement, il pourra mentionner en commentaires de l'évaluation qu'il se réfère la réponse faite par son prestataire dans sa propre annexe.

5. Comment se définit la notion de monnaie électronique à la section I. 6 de l'annexe ?

Cette notion de « monnaie électronique » correspond à la définition donnée par la 2e Directive monnaie électronique (DME2) considérant 8 et article 2, reprise à l'article L. 315-1 du Code monétaire et financier (CMF), soit « une valeur monétaire qui est stockée sous une forme électronique, y compris magnétique, représentant une créance sur l'émetteur, qui est émise contre la remise de fonds aux fins d'opérations de paiement telles que définies à l'article 4, point 5), de la directive 2007/64/CE et qui est acceptée par une personne physique ou morale autre que l'émetteur de monnaie électronique ». Selon l'article 11.2 de la DME 2, « les États membres veillent à ce que les émetteurs de monnaie électronique remboursent, à la demande du détenteur de monnaie électronique, à tout moment et à la valeur nominale, la valeur monétaire de la monnaie électronique détenue ».

Selon cette définition, la valeur monétaire stockée doit en conséquence réunir les quatre conditions suivantes :

- Créance du détenteur sur l'émetteur ;
- Remise de fonds par le détenteur ;
- Acceptation aux fins d'opérations de paiement par le détenteur ;
- Remboursement sur demande du détenteur.