DSP3/RSP : une réforme structurante pour les banques européennes

Emmanuelle CHOUKROUN

Directrice adjointe de l'équipe Relations Interbancaires, Société Générale

Il aura fallu 3 ans pour finaliser le nouveau corpus réglementaire applicable au secteur des paiements, publié en même temps que les propositions de loi sur l'euro numérique et sur l'Open Finance (FIDA). Si les discussions entre co-législateurs sont terminées, la publication des textes définitifs au journal officiel de l'Union européenne est attendue entre juin et septembre 2026.

Ce corpus repose sur deux textes complémentaires :

- La troisième Directive sur les Services de Paiement, dite « DSP3 », détaille le régime prudentiel applicable aux acteurs non-bancaires des paiements. Etablissements de paiement et établissements de monnaie électronique sont désormais régis par un seul et unique texte ;
- Le Règlement sur les Services de Paiement, dit RSP, expose les règles applicables aux Prestataires de Services de Paiement (« PSP »), quel que soit leur statut.

Post-adoption, à quoi ressemblera concrètement la feuille de route d'un établissement de crédit pour se mettre en conformité ?

Des investissements majeurs, dans un calendrier contraint

Disons-le tout de suite : les investissements seront significatifs et concentrés majoritairement sur les moyens de lutte contre la fraude et les dispositions Open Banking. Le calendrier, quant à lui, s'annonce particulièrement serré, l'essentiel des nouvelles obligations entrant en application 21 mois après la publication des textes.

L'enjeu est d'autant plus critique que la fraude aux moyens de paiement continue de progresser. Selon l'Autorité Bancaire Européenne, le montant total des fraudes aux moyens de paiement dans l'Union européenne s'est élevé à 4,2 milliards d'euros en 2024 (contre 3,5 milliards en 2023). Les virements frauduleux concentrent l'essentiel des pertes, 85 % d'entre elles étant supportées par les clients, dans un contexte où les fraudeurs ciblent des opérations unitaires toujours plus élevés[1].

Un cadre renforcé de lutte contre la fraude

Dans le cadre de RSP, les PSP, bancaires ou non, devront déployer un arsenal étendu de dispositifs, qu'il est possible de classer en trois catégories :

- **Les mesures préventives** prévoient notamment
  - l'extension du service de vérification Nom-IBAN à tous les types de virements ;
  - la possibilité pour l'utilisateur d'activer des périodes de temporisation ;
  - l'instauration d'un plafond de dépenses tout en permettant à l'utilisateur de définir une limite de dépense spécifique par instrument de paiement.

1. Source : Rapport conjoint de l'ABE et de la BCE relatif à la fraude sur les moyens de paiement publié en décembre 2025.

Ces dispositions constituent autant de garde-fous supplémentaires face à la fraude par manipulation, contre laquelle l'Authentification Forte s'est révélée peu efficace.

- **Les mesures détectives** reposent sur une surveillance étendue des transactions entrantes et sortantes. Les PSPs auront désormais l'obligation de suspendre une transaction jugée douteuse, sous peine d'avoir à indemniser le client en cas de fraude avérée. Cette obligation ne s'applique pas au virement instantané, pour lequel le PSP devra, en cas de doute, refuser la transaction. Enfin, les PSPs devront partager entre eux les événements de fraude dont ils ont connaissance au travers de plateformes dédiées, utiles pour permettre à l'écosystème de se défendre plus efficacement et de pouvoir qualifier une opération de « douteuse ».

- **Les mesures correctives** dont la plus emblématique est celle posant l'obligation de remboursement de l'usager en cas de fraude par usurpation d'identité du PSP, dès lors que l'un de ses canaux a été compromis et sous réserve d'un dépôt de plainte par l'usager. Par ailleurs, le délai de réclamation est étendu à 18 mois et les PSPs auront le droit d'engager la responsabilité des grandes plateformes ou moteurs de recherche en ligne lorsqu'ils continuent d'héberger du contenu frauduleux après signalement.

Si les obligations pesant sur les PSPs s'alourdissent, les usagers, particuliers ou entreprises, auront également un rôle spécifique à jouer dans la lutte contre la fraude susceptible de les affecter, que ce soit en matière de fixation de limites ou dans les interactions avec la banque en cas de suspension d'opérations suspectes.

Open Banking : des évolutions structurantes

Les investissements des établissements de crédit concerneront également les services d'Open Banking, dont la gratuité pour les utilisateurs est maintenue.
Deux évolutions apparaissent particulièrement structurantes.
La première est l'obligation de mise en place d'API comme interface d'accès au compte, nécessitant un effort d'adaptation important pour les établissements de crédit qui jusqu'ici avaient privilégié des solutions de type « web-scraping » sécurisé.
La seconde concerne la mise en place d'un tableau de bord qui permet à l'utilisateur de gérer les consentements donnés aux tiers, et notamment de les retirer, renforçant ainsi le contrôle des usagers sur leurs données.
D'autres développements sont également prévus mais relèvent plus de l'affinage du cadre précédent que de nouveautés réelles, sans être neutres en termes d'effort opérationnel (publication de statistiques sur les initiations de paiement réussis, suivi des indisponibilités planifiées ou non, etc.).

Information des usagers et droit au compte

Enfin, le panorama ne serait pas complet sans évoquer les impacts liés au renforcement des obligations d'information des usagers et ceux liés à la consécration du droit au compte de paiement pour les établissements de paiement et de monnaie électronique.
Le premier item appelle à une **révision des documents contractuels et parcours clients** ainsi qu'à des adaptations IT importantes pour assurer les informations requises, notamment sur les frais applicables et en lien avec les informations sur le change.
Le second génère un risque accru de contentieux ou de recours devant l'autorité compétente et nécessitera un effort considérablement augmenté de documentation et de justification en cas de refus d'ouverture de compte pour les établissements de crédit.

Conclusion

Les établissements de crédit demeurent des acteurs clés dans l'écosystème des paiements. A ce titre, ils sont fortement sollicités, tant pour renforcer la lutte contre la fraude que pour accompagner la modernisation de l'économie.
Pour autant, la multiplication des obligations imposées aux banques – notamment l'obligation de fournir des services gratuitement ou à prix administré, souvent sans maîtrise de leur périmètre ni de leur modèle économique, qu'il s'agisse de l'Open Banking, de la confirmation systématique Nom/IBAN ou de dispositifs analogues – doit désormais faire l'objet d'un débat lucide. Non sur leur principe, mais sur leurs effets cumulatifs.

À défaut, le risque est clair : fragiliser progressivement les capacités d'investissement d'un secteur clé pour contribuer à financer et sécuriser l'Europe numérique. Or une stratégie européenne ambitieuse en matière de paiements, de digitalisation et de souveraineté ne peut durablement reposer sur des acteurs privés sommés d'investir toujours davantage tout en voyant leur capacité de création de valeur se réduire. ■