Lutte contre la fraude : banques et fintechs se préparent à collaborer au niveau européen

● Actuellement en discussion au niveau européen, la version finale de la future directive sur les services de paiement (DSP3), et du règlement qui l'accompagne, est attendue pour la fin de l'année.
● Ses impacts seront majeurs, sur la lutte contre la fraude notamment.

BANQUE

Tifenn Clinkemaillié

Gouvernement démissionnaire ou pas, l'agenda européen suit son chemin. Et dans le domaine des paiements, plusieurs échéances approchent. Au cœur de l'été, banques, prestataires de services de paiement et direction du ministère de l'Economie et des Finances se sont réunis pour travailler à la mise en place de l'une d'elles : la DSP3, nouvelle version de la directive sur les services de paiements, et du règlement sur les services de paiement (PSR) qui l'accompagne.

Une seconde réunion est prévue au cours du mois de septembre. Objectif : anticiper le vote de ces textes par Bruxelles. Alors que la Commission a présenté ses ambitions fin juin 2023, les versions finales de la directive et du règlement sont attendues pour la fin de l'année. Leurs mises en application devraient, elles, intervenir d'ici à 2026. Et l'enjeu est important, dans le cadre de la lutte contre la fraude notamment.

Escroqueries plus sophistiquées

Près de dix ans après l'élaboration de la précédente directive sur le sujet (DSP2) – qui a marqué l'entrée en vigueur de l'authentification forte « à double facteur » – le paysage du paiement s'est radicalement transformé. Les fintechs se sont multipliées. Et la fraude est devenue plus sophistiquée. D'où la volonté de Bruxelles de renforcer son arsenal, en faisant notamment travailler ensemble les acteurs de la chaîne.

Banques et prestataires de services de paiement devraient, à terme, pouvoir partager entre eux les informations relatives à la fraude, comme les numéros d'IBAN utilisés par les escrocs. Reste pour les régulateurs nationaux à déterminer la liste exacte des informations qui pourront transiter.

Cadre légal de partage de données

Surtout, le texte établit un cadre légal pour le partage de ces informations. Et place la lutte contre la fraude comme intérêt supérieur à la protection des données. Une avancée réclamée par les acteurs du secteur, qui se voyaient parfois contraints par le RGPD, le texte réglementaire européen qui encadre le traitement des données, ou le respect du secret bancaire. *« La fraude est partout, et pour créer un écosystème de paiement qui est fonctionnel, le mieux c'est qu'on collabore tous ensemble »*, souligne Fanny Rodriguez, secrétaire générale et directrice des opérations de Fintecture, start-up spécialisée dans le paiement par virement.

Les acteurs du paiement pourraient ne pas être les seuls concernés. *« Il faut intégrer toutes les parties de la chaîne, des opérateurs de télécommunications aux plateformes de l'e-commerce,* avance Corina Fontaine, vice-présidente de France Payments Forum, association représentant les acteurs de l'industrie du paiement. *La Commission est en train de travailler pour voir comment elle pourrait les inclure dans cette directive ».*

> « Il faut intégrer toutes les parties de la chaîne, des opérateurs de télécommunications aux plateformes de l'e-commerce. »
> **CORINA FONTAINE**
> Vice-présidente de France Payments Forum

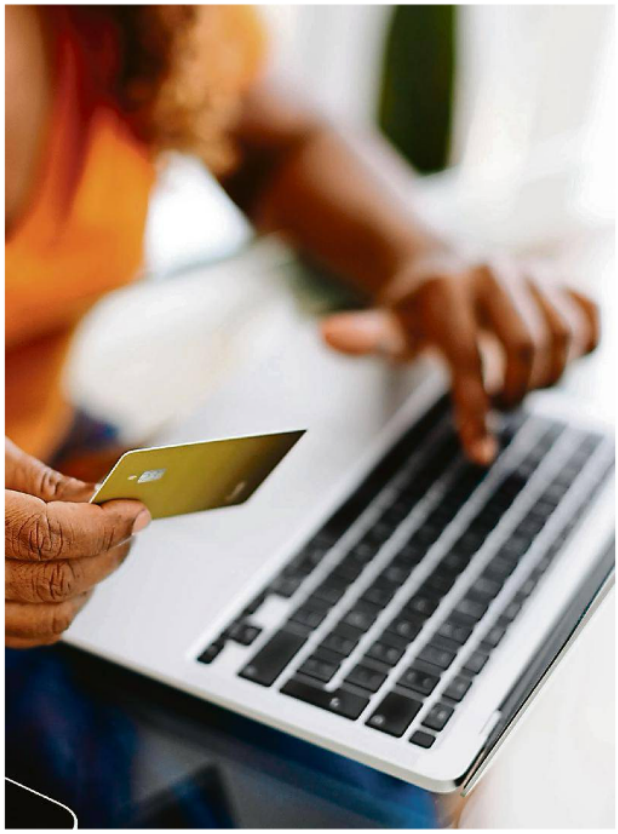
Le règlement clarifie par ailleurs la responsabilité de chacun en cas de fraude. Jusqu'à présent, celle-ci reposait d'abord sur la banque, qui pouvait elle-même se retourner contre le prestataire de services de paiement. *« Là, il y a clairement écrit que chacun est responsable de son propre périmètre »*, analyse Fanny Rodriguez, qui est aussi membre de l'association des établissements de paiements (AFEPAME).

Autre avancée importante : banques et fintechs devront vérifier systématiquement la concordance entre l'IBAN et le nom du bénéficiaire d'un transfert de fonds. L'authentification forte serait rendue obligatoire sur davantage d'usages, comme l'enrôlement d'une carte de crédit dans un portefeuille électronique, l'abonnement et tous les types de virement. Et à la différence de la DSP2, ces règles sont inscrites dans un règlement, qui s'applique sans divergences d'interprétations possibles au sein de l'UE.

Protéger le consommateur

Enfin, la protection du consommateur restera un enjeu. Le règlement devrait préciser les conditions sous lesquelles les victimes pourront être remboursées. Selon la version de la Commission, publiée en juin 2023, les banques seront tenues de restituer les sommes dérobées notamment si le fraudeur s'est fait passer pour l'un de leurs employés en usurpant leur numéro de téléphone ou leur adresse e-mail.

Mais les travaux se poursuivent. Le texte devrait notamment définir dans le détail la notion « d'ingénierie sociale », pratique de manipulation psychologique réalisée à des fins d'escroquerie, que les clients invoquent pour se faire rembourser, mais aussi de « négligence grave » des clients, régulièrement mise en avant par les banques pour ne pas les rembourser. *« Le règlement dit qu'il faut que les acteurs renforcent les mécanismes face à l'ingénierie sociale, mais aujourd'hui les banques ne peuvent pas lutter contre un fraudeur qui s'approprie leur nom*, souligne Géraldine Grandmougin, responsable de la conformité réglementaire pour le cabinet de conseil spécialisé dans les paiements, Oaklen consulting. *Ces notions sont en cours de discussion ».* ■



Le texte place la lutte contre la fraude comme intérêt supérieur à la protection des données. Une avancée réclamée par les acteurs du secteur. *Photo Shutterstock*

De l'« open banking » à l'« open finance » : Bruxelles veut accélérer l'ouverture des données bancaires

En révisant sa directive sur les paiements (DSP3), et en lui associant un règlement, l'Union européenne prévoit d'harmoniser les règles régissant l'accès aux données bancaires. De nouvelles contraintes pèseront sur les banques, à l'avantage des fintechs.

Protéger le consommateur contre la fraude… tout en favorisant l'innovation et le développement de nouveaux services. En révisant sa directive sur les paiements (DSP3), en juin 2023, et en lui associant un règlement (PSR), texte juridique qui s'applique de manière uniforme et obligatoire dans les 27 Etats membres, la Commission européenne s'est fixé un double objectif ambitieux.

Ce dernier est en passe de se concrétiser. Si les discussions se poursuivent à Bruxelles, les versions finales des deux textes sont attendues pour la fin de l'année. Les fintechs s'imposent comme en étant les principales bénéficiaires, grâce à la mise en place d'un cadre clair régissant l'accès aux données bancaires (« open banking »).

Des freins qui subsistent

A l'origine de cette réglementation, un constat : la précédente directive sur les services de paiement (DSP2), publiée en 2015 et qui avait posé les bases de l'« open banking », n'est pas appliquée de manière uniforme au sein de l'Union. Et ces différences pénalisent les prestataires de services de paiement, dont les fintechs, pourtant directement nés de la DSP2 et de la volonté de l'Europe de les favoriser.

« De nombreux freins subsistent pour les fintechs, décrypte Thierry Leblond, responsable du conseil en paiement pour le cabinet spécialisé Oaklen consulting. *Elles reprochent notamment aux banques de ne pas fournir toutes les informations ou de ne pas faciliter les parcours clients ».* Les interfaces (API) pour avoir accès à ces informations sont aussi pointées du doigt. *« Tout est à la discrétion des banques ou du régulateur local, il y a donc des pays où cela fonctionne bien, et d'autres endroits où la performance est très disparate »*, abonde Anjan Som, directeur technique et cofondateur de Fintecture, start-up spécialisée dans le paiement par virement.

Sanctions lourdes

L'ambition de Bruxelles est d'apporter de l'harmonie, non seulement sur le fond, en listant les données qui devront obligatoirement être transmises par les banques, mais aussi sur la forme, avec des interfaces standardisées et gratuites. Surtout, les banques pourront être sanctionnées si elles ne jouent pas le jeu.

La DSP3 offre ainsi la possibilité aux prestataires de services de paiement de signaler les mauvais élèves à l'autorité de contrôle locale, à l'instar de l'ACPR en France. Et les sanctions devraient être lourdes. *« Elles pourraient atteindre jusqu'à 7,5 % du chiffre d'affaires, mais l'objectif est clairement de ne pas y recourir, et de pousser les banques à jouer le jeu »*, détaille Géraldine Grandmougin, responsable de la conformité réglementaire pour Oaklen consulting.

Priorité est aussi donnée à l'information des consommateurs. Le client devrait ainsi avoir accès en permanence à un tableau de bord lui permettant de savoir avec quel établissement il partage ses informations financières et lesquelles il partage exactement.

Et à ce règlement s'en ajoute un autre. Baptisé « Fida », et présenté en juin 2023, il ambitionne de passer de l'open banking à l'open finance. Le texte prévoit pour cela de poser un cadre d'accès aux données financières, comme les informations d'épargne, de crédit ou d'assurance-vie. Si les discussions se poursuivent au niveau européen, les questions avant une éventuelle adoption restent, pour le moment, nombreuses. — *T. C.*

Le Royaume-Uni revoit sa copie

L'autorité britannique chargée des systèmes de paiement revoit à la baisse le montant maximal que les établissements financiers vont devoir rembourser à leurs clients en cas de « fraude au paiement push autorisé ».

Ingrid Feuerstein

Après des mois de bras de fer avec le secteur financier, le régulateur britannique a finalement battu en retraite sur son nouveau régime de remboursement des victimes de fraudes au paiement. Selon le « Financial Times », le PSR (« Payment Systems Regulator »), l'autorité britannique chargée des systèmes de paiement, va revoir à la baisse le montant maximal que les établissements financiers devront rembourser à leurs clients en cas d'escroquerie.

Ce plafond se situera finalement à 85.000 livres, soit un niveau bien inférieur au montant de 415.000 livres initialement envisagé. Prévu pour entrer en vigueur le 7 octobre, ce régime doit contraindre les banques et autres acteurs du paiement britanniques à dédommager systématiquement leurs clients victimes de « fraude au paiement push autorisé » (APP), c'est-à-dire quand ils ont été manipulés pour effectuer des paiements en temps réel aux fraudeurs. Il s'inscrit dans le cadre d'un vaste arsenal antifraude adopté par le Royaume-Uni post-Brexit. Parmi les autres mesures envisagées, figure l'allongement des délais accordés aux banques pour valider une transaction en cas de « paiement push » sur un mobile.

L'obligation de remboursement à 415.000 livres avait déclenché une levée de boucliers du secteur financier, qui y voyait une brèche à exploiter pour la criminalité financière et une barrière à l'entrée pour les fintechs. Annoncée en décembre 2023, la réforme avait suscité un tel tollé que le directeur du PSR, Chris Hemsley, avait été contraint de quitter ses fonctions début juin.

Son remplaçant par intérim, David Geale, avait néanmoins affiché sa volonté d'aller au bout de ce projet, rappelant la nécessité *« d'agir rapidement »*. En 2023, la fraude au paiement push autorisé a coûté près de 460 millions de livres aux Britanniques.

« Décision pragmatique »

Les lobbys financiers, jugeant le plafond de remboursement trop élevé, demandaient qu'il soit abaissé à 30.000 livres. Les professionnels souhaitaient en outre un délai supplémentaire pour mieux se préparer à cette échéance.

UK Finance, l'association représentant les banques britaniques, a accueilli favorablement l'abaissement du seuil à 85.000 livres, saluant *« une décision pragmatique »*. Cette limite *« couvre encore la quasi-totalité des cas de fraude APP, de sorte que la majorité des victimes seront toujours protégées si le plafond est réduit »*, a réagi son porte-parole Andy Donald.

Selon un rapport du PSR publié en août, ces fraudes au paiement push autorisé ont fait l'objet d'un remboursement dans 67 % des cas seulement en 2023. Un chiffre certes en hausse par rapport à 2022, où il atteignait 61 %, mais qui cache de grandes disparités selon les établissements bancaires. Parmi les bons élèves, le régulateur citait Nationwide, TSB et Barclays, qui remboursent leurs clients dans plus de 80 % des cas. A l'inverse, ces fraudes ont été indemnisées dans seulement 3 % des cas chez AIB, 7 % chez Danske Bank et 9 % chez Monzo. ■