



Fusion et scission du cadre légal sur les services de paiement (à propos de la DSP3)

La proposition, publiée le 28 juin 2023 par la Commission européenne, de refonte du cadre légal gouvernant les services de paiement (qui incluent dorénavant la monnaie électronique) et leurs utilisateurs et prestataires, consiste d'abord à fusionner deux directives historiques : la directive de 2009 sur la monnaie électronique (DME2) et la directive de 2015 sur les services de paiement (DSP2). Elle consiste ensuite à scinder des véhicules législatifs, en décidant :

- De soumettre à une directive (d'harmonisation maximale), qu'on peut désigner comme la DSP3 (PSD3 en anglais), les sujets d'agrément et de surveillance des établissements de paiement (les « EP », qui incluent désormais les établissements de monnaie électronique) ; et
- De soumettre à un règlement (d'application directe) qu'on peut désigner comme le RSP (PSR en anglais) les sujets de transparence des conditions et des exigences en matière d'information en ce qui concerne les services de paiement/de monnaie électronique et les droits et obligations respectifs de leurs prestataires et utilisateurs.

La Commission a justifié cette scission par la trop grande fragmentation des transpositions nationales sur les services de paiement/monnaie électronique, tandis que l'agrément et la surveillance des prestataires de ces services s'accommode mieux d'une directive dès lors que l'agrément et la supervision restent attachés aux prérogatives des États membres.

Au-delà de la « cuisine » législative, qui inclut également un règlement cadre sur l'accès aux données afin de rapprocher le cadre légal sur les services de paiement des exigences du RGPD, ce qui interpelle

les praticiens des services de paiement, ce sont les attentes de la Commission sur différents sujets, qu'on peut identifier dans le PSR :

- l'assouplissement du système d'authentification forte, notamment pour favoriser l'inclusion des « décrochés » du numérique (personnes en situation de handicap, personnes âgées, etc.), qui n'ont pas forcément l'utilisation de smartphones ;
- la dispense d'authentification forte pendant une période de 180 jours suivant une telle authentification, pour les prestataires d'information sur les comptes ;
- un fondement juridique pour l'échange d'informations sur la fraude entre acteurs des services de paiement ;
- l'extension à tous les virements en devises de l'UE du service de vérification de l'IBAN (cohérence du couple IBAN/bénéficiaire), sachant que ce service est déjà rendu obligatoire pour les virements instantanés dans la proposition de règlement sur les virements instantanés ;
- l'inversion possible de la responsabilité en cas de fraude dans les situations de paiement initiés par les commerçants (*Authorised Push Payments*) et une possible prise en charge de la fraude sur les virements par le prestataire de services de paiement du bénéficiaire.
- l'extension de l'interdiction historique du *surcharging* aux opérations libellées dans une devise autre que l'euro ;
- le renforcement de la protection du consommateur sur les remboursements liées aux transactions initiées par des marchands ;
- l'obligation pour les banques de mettre à disposition de leurs client un tableau de bord leur permettant de révoquer (ou réactiver) l'autorisation donnée à un fournisseur de services d'*open banking* d'accéder à ses données ;
- le renforcement de l'information des consommateurs sur les modalités de traitement de leurs réclamations ;
- le renforcement des superviseurs sur le pouvoir d'interdire temporairement la vente de certains produits de paiement.

Alors que la Commission a renvoyé à une consultation à venir en 2024 le soin d'élargir l'*open banking* vers l'*open finance*, elle tend à uniformiser les règles, sans pour autant interdire la subsistance de règles nationales plus protectrices¹, spécifiquement sur :

- la transparence des conditions et exigences en matière d'informations régissant les services de paiement ; et
- les droits et obligations liés à la prestation et à l'utilisation des services de paiement.

Dans ce cadre, le GT RED a souhaité détailler les enjeux des évolutions sous-jacentes à ces deux grandes thématiques, à travers l'évolution :

1. de l'*open banking* ;
2. du champ d'application matériel et territorial ;
3. de la protection du consommateur (frais, situations des opérations hors UE, blocage des fonds) ;
4. de la sécurité et la prévention de la fraude ;
5. de la pratique *de-risking* ;

¹ La Commission accepte donc que la fragmentation du marché continue d'exister malgré sa décision d'adopter un Règlement.

Nous examinons ci-après ces cinq thématiques avec l'espoir de convaincre le législateur européen (le Conseil et le Parlement européen) d'améliorer les grandes tendances initiées par la Commission par le PSR.

1. Open Banking

Avec le PSR, la priorité est donnée à l'*Open Banking*, plutôt qu'à l'*Open Finance*, renvoyé à un autre véhicule législatif. Les mesures prévues par le nouveau texte constituent toutefois un axe fort de la réforme. Ayant tiré les meilleures leçons de la DSP2, dont la mise en place des API s'est faite d'une manière très hétérogène avec un cadre technique global spécifique à chaque pays (Berlin Group, STET, etc.), la Commission vise avec cette nouvelle réforme à réduire toutes les frictions existantes.

Les éléments-clé des mesures du PSR demeurent la qualité, la standardisation et l'adoption des API, pour permettre l'interopérabilité et le rapprochement entre les banques et les prestataires non bancaires concernés (établissements de paiement, établissements de monnaie électronique et prestataires tiers).

Dans ce cadre, les banques sont incitées à fournir des APIs de qualité, facilitant ainsi la normalisation de fonctions d'échange, avec des temps de réponses rapides et des gestions multiples de bénéficiaires. Cela implique un engagement fort de la part des banques, avec des publications régulières sur les API des disponibilités et des performances, et l'anticipation de changements techniques trois mois à l'avance. En cas de dysfonctionnement et de non accès aux API qui leur sont dédiées, les TPP pourront être autorisés à demander à leur autorité compétente nationale (en France l'ACPR) de pouvoir utiliser l'interface que la banque (ASPSP) fournit à ses clients jusqu'à ce que l'API spécifique soit à nouveau disponible.

Pour des considérations de concurrence, les banques se voient aussi imposer un devoir d'information auprès des établissements de paiement (EP) et établissements de monnaie électronique (EME) sur les situations d'échec à l'accès aux comptes et à l'initiation. Pour compléter ces mesures, l'ACPR bénéficiera d'un pouvoir de supervision et de sanction.

À noter aussi, une nouvelle obligation pour les ASPSP de mettre un tableau de bord (*Dashboard*) à disposition de leurs clients. Ce tableau de bord permettra aux clients de suivre les autorisations données aux TPPs pour accéder à leurs données avec un historique de deux ans. Les clients finaux pourront révoquer et réactiver leurs autorisations en temps-réel. Ce dispositif va dans le sens d'une meilleure sécurisation de l'*Open Banking* pour le consommateur.

Enfin, le PSR prévoit un chapitre complet sur l'authentification forte (SCA), avec en particulier une extension de 90 à 180 jours du délai entre deux authentifications fortes.

Dans cette perspective, l'*Open Banking* bénéficie à tout l'écosystème. À titre d'exemple les bénéfices se répartissent différemment pour :

- Les banques, qui vont endosser plus facilement le rôle de Tiers de Confiance, basé sur un nouveau modèle innovant dans une optique de réduction de coûts ;
- Les PSP, dans un contexte où l'évolution européenne apporte un coup d'accélérateur pour les acteurs non bancaires et le développement des services à valeur ajoutée ;
- Les autorités de supervision, qui auront une meilleure capacité de contrôle et de traitement de la fraude dans les paiements, avec un soutien dans l'innovation et de l'écosystème des EP/EME ;
- Les clients, qui bénéficient de services à valeur ajoutés, avec un accès à un marché concurrentiel et une personnalisation des offres.

AVIS du GT RED du FPF

Avec l'*Open banking*, une réelle accélération est donnée à l'**harmonisation de l'espace UE des paiements**. Ce nouveau cadre élargit le concept de banque ouverte, permettant ainsi un accès plus large aux données. Les règles de partage d'informations entre Banques et PSP sont renforcées et le champ d'action des superviseurs étendu.

Toutefois, toutes ces exigences impacteront fortement les banques, avec des changements importants dans leurs systèmes d'information, qui seront inévitables pour continuer à développer les services, à fournir des interfaces dédiées (API) et à adopter de nouvelles technologies pour suivre toutes les évolutions et exigences réglementaires.

2. Champ d'application matériel et territorial

Alors que la DSP2 contenait une disposition limitée au champ territorial des règles, le PSR refond le texte pour y inclure le champ matériel, qui reprend notamment mais pas seulement l'ancienne liste des activités exclues du champ d'application.

2.1 Champ territorial

Pour l'essentiel, il est inchangé par rapport à la DSP2 :

- l'ensemble des règles s'applique aux opérations à deux jambes si la monnaie stipulée est issue de l'Espace économique européen (EEE) (les deux PSP sont dans l'EEE) ; une part de ces règles s'applique si la monnaie est hors EEE ; et
- un corpus de règles plus réduit est applicable aux opérations à une jambe (un seul des deux PSP impliqués est situé dans l'EEE), peu importe que l'opération soit libellée dans une monnaie de/hors EEE.

Cela étant rappelé, on peut regretter que le contenu des règles applicables résulte toujours d'une énumération en creux (« règles applicables sauf »), qui n'est pas propice à la compréhension globale de ce qui est fondamentalement attendu des PSP concernés.

On remarquera plus simplement que le PSR augmente les exigences des PSP en matière de transparence et d'obligations sur l'exécution de l'opération de paiement et que le renforcement des exigences rejaillit mécaniquement sur les opérations (i) en monnaies autres que celles de l'EEE ou (ii) « à une jambe ».

On peut observer que dans ses travaux préliminaires sur la révision de la DSP2, la Commission avait remarqué avoir reçu très peu de commentaires sur la nécessité de faire évoluer le champ territorial, ce qui peut s'expliquer par une certaine méconnaissance des enjeux et risques pratiques y associés.

On doit également noter que la Commission est consciente des risques de contournement des règles européennes, particulièrement lorsqu'elle évoque les situations de contournement de l'obligation d'authentification forte dans le commerce en ligne. Elle pose ainsi le principe que l'exigence ne peut être « *contournée par des pratiques telles que le recours à un acquéreur établi en dehors de l'Union en vue d'échapper aux exigences en matière d'authentification forte du client* ».

Enfin, on peut regretter que le champ d'application n'évolue pas pour tenir compte des opérations de conversion en cryptoactifs alors qu'on aurait pu attendre du PSR qu'il s'applique à coordonner les nouvelles règles issues du règlement européen concerné (MiCA) sur (i) des opérations de conversion

de monnaie fiat en crypto actifs et réciproquement (où une jambe porte sur des monnaies de l'EEE et l'autre jambe sur des cryptoactifs) et (ii) sur les règles applicables aux opérations portant sur des jetons de monnaie électronique (selon la terminologie MiCA), dont on peine à comprendre s'ils sont complètement assimilables à de la monnaie électronique.

On peut espérer que ces efforts de clarifications seront entrepris par le Parlement européen et le Conseil en vue de l'adoption du règlement.

AVIS du GT RED du FPF

Le Parlement européen et le Conseil devraient s'attacher à mieux coordonner le PSR avec les interactions que les paiements et la monnaie électronique peuvent avoir avec les cryptoactifs du Règlement MiCA, particulièrement les jetons de monnaie électronique, dont on comprendrait mal que le champ territorial ne suive pas les principes énoncés par le PSR.

2.2 Champ matériel

La DSP2 avait ouvert le champ matériel aux prestataires d'informations sur les comptes et aux initiateurs de services de paiement.

Le PSR fait d'abord évoluer la notion d'établissement de paiement pour y inclure les établissements de monnaie électronique. Malheureusement, même si les acteurs concernés appliqueront de façon générale les nouvelles règles, la difficulté de différencier monnaie électronique et services de paiement subsiste nécessairement à travers les règles nationales d'assimilation entre espèces et monnaie électronique. Par exemple, la France assimile pour partie la monnaie électronique non anonyme aux espèces et plafonne ainsi son utilisation à des niveaux très bas (3.000 € pour les résidents, 10 ou 15.000€ pour les non-résidents selon le bénéficiaire du règlement) alors que de telles restrictions ne sont nullement opposables à des règlements via des établissements de paiement. En outre, on peut s'interroger sur la question de savoir si les règles nationales de plafonnement des règlements en espèces ou en monnaie électronique s'appliqueront de la même manière aux jetons de monnaie électronique du règlement MiCA.

Le PSR fait ensuite évoluer à la marge le régime des exclusions ; il entend par exemple déléguer à la Commission le soin de définir dans des normes techniques de réglementation (RTS) les limites des régimes d'exemptions, notamment celui associé au « réseau limité d'accepteurs » ou l'« éventail limité de biens et services » (*limited network exemption*), qui figure aujourd'hui dans des orientations de l'Autorité bancaire européenne (EBA).

Sur ce régime d'exclusion, on peut s'interroger sur la tendance expansionniste de certaines autorités nationales (y compris l'ACPR) en matière d'encaissement de fonds pour compte de tiers sur des prestations rendues dans des secteurs où on les attend moins, soit parce que les opérations de paiement réalisées ne concernent pas les consommateurs, soit parce qu'elles obéissent historiquement à un cadre social fort assimilable aux titres spéciaux de paiement. C'est notamment le cas du marché du tiers-payant associé au remboursement des frais de santé, dans lequel l'ACPR refuse de considérer (i) que les acteurs concernés relèvent du régime de l'exemption d'agrément et (ii) que les prestataires de santé considérés puissent déléguer le règlement des dépenses de santé à des acteurs tiers dans le cadre d'accords de sous-traitance.

Le PSR entend également s'assurer que certains des régimes d'exclusion soit contraint par des lignes directrices, tel que l'exclusion de l'« agent commercial », qui a fait débat en France lorsque les places

de marché ont été forcées par l'ACPR à prendre le statut d'établissement de paiement ou d'agent de ces derniers.

Le PSR fait aussi rentrer les prestataires de services techniques dans le champ de certaines exigences, même s'il les fait apparaître dans le régime des exclusions. Cette évolution est notamment liée, selon le rapport sur la DSP2, à l'apparition de portefeuilles électroniques (les *pass-through wallets*) qui permettent, grâce à la tokenisation, d'utiliser un instrument de paiement via un appareil mobile pour effectuer des paiements en ligne ou sans contact² et même proposer des services novateurs tels que *buy-now-pay-later* (BNPL) ou le *request-to-pay* (RTP). Or les fournisseurs de ces services techniques sont exclus du champ d'application de la DSP2. Pourtant ces fournisseurs sont parfois les opérateurs de systèmes de paiement ou des grands processeurs de données de paiement qui ont acquis un statut quasi-systémique dans certains États membres (cela inclut notamment les GAFAM). C'est dans ce cadre que le PSR impose à ces prestataires certaines exigences applicables aux PSP, particulièrement dans leur déploiement des solutions d'authentification forte.

On peut s'interroger sur la limitation des exigences, même s'il faut remarquer que ces prestataires de services techniques seront à terme soumis à des règles sur la sous-traitance plus ou moins forte en fonction de leur implication dans l'accomplissement des services techniques et que dans le déploiement des infrastructures de paiement, ils relèvent de règles issues de la Banque Centrale Européenne (BCE).

Dans la même veine, on relève également la prise en compte dans le PSR d'acteurs qui ne relèvent pas du secteur financier, lorsqu'ils concourent à l'émergence du marché de niche de la distribution d'espèces.

On remarque enfin la suppression des exclusions historiques de ce qu'on appelle en France les changeurs manuels ou les transporteurs de fonds.

AVIS du GT RED du FPF

Comme pour le champ territorial des règles sur le paiement, la version finale du PSR devrait définir le champ matériel des règles en coordonnant mieux celles-ci avec les règles applicables aux cryptoactifs (issues de MiCA) afin que les utilisateurs des moyens de paiements ou de cryptoactifs assimilables à de la monnaie électronique (cf. les jetons de monnaie électronique) connaissent les règles applicables.

Sur les régimes d'exclusion, le PSR gagnerait à mieux traiter le sujet de l'encaissement de fonds pour compte de tiers (qui n'a fait l'objet de clarifications par la Commission qu'en janvier 2023), en permettant notamment aux États membres de reconnaître à certains acteurs déjà réglementés le droit d'externaliser ces services à des prestataires de services techniques qui restent sous leur contrôle.

3. Protection du consommateur

Pratique du surcharging

La pratique consistant à imposer des frais supplémentaires pour l'utilisation d'un instrument de paiement donné est parfois connue sous le vocable anglophone de *surcharging*. Sous la DSP2, l'interdiction du

² On a notamment perçu l'importance de cette qualification dans une position de l'ACPR de septembre 2019 sur le service d'acquisition d'ordres de paiement, les prestataires techniques intervenant en amont ou en aval de ce service n'étant pas concernés par l'obligation d'agrément en tant que PSP.

surcharging relevait d'un corpus minimum de règles avec une large latitude laissée aux Etats membres de renforcer l'interdiction de contourner le règlement sur les commissions interchange (paiement trois ou quatre coins, y compris Paypal) ou celles figurant dans les règles SEPA (virements et prélèvements).

Les nouvelles règles visent de façon générale à aligner les traitements de l'ensemble des opérations initiées par le bénéficiaire (Prélèvements vs. Opérations dites *MIT*).

Ensuite, le PSR vise à inclure dans le régime anti-contournement précité les contraintes dictées par le (futur) règlement sur le virement instantané. Mais surtout, le PSR étend non seulement l'interdiction du *surcharging* aux virements/prélèvements transfrontaliers dans l'UE (SEPA) mais aussi aux opérations hors Règlement SEPA.

Il reste à déterminer si les Etats membres useront de la possibilité qui subsiste dans le PSR d'adapter le régime national du *surcharging*. Pour mémoire, le législateur français avait clairement choisi d'interdire la pratique du *surcharging* (cf. articles 112-11 et suivants du Code monétaire et financier), sans préciser si des dérogations étaient contractuellement opposables au secteur B2B. On peut espérer que la distinction entre moyens de paiement *Corporate* et moyens de paiement *Consommateur* sera mieux traitée dans le cadre des futures règles nationales, afin de laisser place à davantage de concurrence sur ce terrain du commerce B2B.

Règles sur les opérations hors Espace économique européen (EEE)

Le PSR vient combler un manque criant de transparence des opérations de paiement hors EEE, dans un contexte où le Règlement visant à uniformiser les règles concernant les paiements transfrontaliers dans l'UE ne traite non seulement pas des virements hors EEE mais ne traite pas non plus de la situation spécifique de la transmission de fonds (transfert d'argent, en anglais *remittance*).

Au-delà de la question de la conversion dans des devises hors EEE, éminemment importante, celle du délai d'exécution était également mal appréhendée par la DSP2. Le règlement vise donc à mieux protéger les intérêts des utilisateurs européens dans ces situations d'opérations exécutées hors EEE, sans aller jusqu'à imposer un délai maximum d'exécution, dans la mesure où ce délai peut fortement dépendre d'impondérables liés à la jambe de la transaction située hors EEE, concernant des prestataires de paiement qui n'ont pas à subir une législation européenne qui ne leur est pas opposable.

Exemption Telco

On peut remarquer dans le PSR l'absence de modification du régime de l'exemption *Telco* (désigne essentiellement les opérations de paiement réglées par le biais de la facture de l'opérateur téléphonique pour l'achat de contenus numériques et de services vocaux) dont la Commission indique ne pas avoir reçu d'indication selon laquelle les utilisateurs de services de paiement via les opérateurs téléphoniques seraient mal protégés. Tout juste peut-on regretter une absence d'augmentation des plafonds prévus sous la DSP2 (de 50€ par transaction et 300€ par mois), compte tenu notamment de la remontée de l'inflation depuis 2022. L'absence d'indexation dans le PSR tend à ralentir le développement de cette activité du secteur du paiement.

On peut penser que le législateur européen augmentera ces seuils en réponse à la demande des opérateurs concernés, qui œuvrent aujourd'hui efficacement à la protection de leurs clients dans le cadre de réglementations nationales convenues au sein de cette profession (en France, on pense ainsi aux recommandations déontologiques de l'Af2m).

Blocage des fonds

On sait que pour les opérations de paiement pour lesquelles le montant de l'opération n'est pas connu à l'avance (ex : réservation d'hôtel, location de voiture ou achat de carburant), les PSP des payeurs peuvent être amenés à bloquer des provisions disproportionnées qui peuvent ensuite obérer la capacité de leurs clients d'utiliser leurs cartes de paiement sur de nouvelles opérations. C'est pour prévenir ces situations que le PSR vise à limiter ces blocages à la fois (i) dans le temps et (ii) dans la proportion du montant bloqué.

Le PSR ajoute ainsi l'obligation (i) du PSP du payeur de contenir le blocage à un niveau proportionné à ce à quoi le « *payeur peut raisonnablement s'attendre* » et (ii) du bénéficiaire d'informer son propre PSP du montant effectivement payé, immédiatement après livraison du service ou des biens au payeur. Le PSP du payeur devra ensuite débloquer les fonds immédiatement à « *réception des informations sur le montant exact de l'opération de paiement* », plutôt que « *après réception de l'ordre de paiement* »

Compte tenu de ces évolutions, on peut s'interroger sur les modalités de transmission au PSP du payeur du niveau proportionné de provision à bloquer alors que cette information n'est par définition connue qu'au moment où le client payeur a fini de profiter de sa réservation d'hôtel ou de voiture.

AVIS du GT RED du FPF

Le Parlement européen et le Conseil devraient œuvrer à mieux préciser certains aspects des propositions de la Commission sur :

- la pratique du *surcharging* ;
- les opérations de paiement hors EEE ;
- l'exemption Telco ;
- le blocage des fonds.

4. Sécurité et prévention de la fraude

Assouplissements de l'authentification forte (SCA)

On relève que le PSR propose une évolution assez majeure pour la SCA : l'authentification forte peut être acceptée comme la composante de deux éléments appartenant à une même catégorie (possession, connaissance ou inhérence), « *pour autant que leur indépendance soit totalement préservée* ».

Cela semble contraire à des avis de l'EBA selon lesquels les deux éléments d'authentification pour SCA doivent appartenir à deux catégories différentes. Cependant l'EBA semble être revenue sur sa position dans les Q&A de 2020, soulignant que les RTS de l'EBA exigent l'indépendance des éléments d'authentification mais pas nécessairement leur appartenance à des catégories distinctes.

L'argument avancé est de ne pas restreindre l'innovation, le développement et l'adoption de nouveaux éléments qui, bien qu'ils entrent dans la même catégorie, répondent à toutes les exigences de sécurité et d'indépendance des RTS de l'EBA.

En clair, sera acceptée une authentification à deux éléments de même catégorie, si ces éléments sont indépendants, comme par exemple :

- Pour la « connaissance » : mot de passe de web-banking et token unique ;
- Pour la « possession » : mobile (numéro) et ordinateur habituel (adresse IP/MAC) ;
- Pour l'« inhérence » : reconnaissance du visage et puce RFID sous la peau.

Position Paper PSR

Rédigé par : GT RED France Payments Forum

Auteurs : Marie-Laure Plessis, Alexandre Marion, Ludovic Vathelot et Corina Fontaine

Octobre 2023

Vérification de la concordance IBAN/Nom du bénéficiaire

Pour sécuriser les paiements et notamment les virements, le PSR prévoit la vérification de la correspondance entre l'IBAN et le nom du bénéficiaire par le PSP du donneur d'ordre, dans la continuité de la proposition de la Commission pour le règlement sur le virement instantané SEPA. L'objectif visé est de donner au donneur d'ordre une indication d'une fraude potentielle ou d'une mauvaise saisie de l'IBAN avant l'exécution du virement.

Les grandes lignes de ce nouveau service sont les suivantes :

- Il concerne les virements SEPA et internationaux,
- Il devra être proposé aux particuliers aussi bien qu'aux entreprises,
- Il pourra être PAYANT (bien que comme le souligne la commission dans son étude d'impacts, il est généralement proposé gratuitement aux particuliers),
- La demande de vérification de la correspondance IBAN/nom effectuée par le PSP du bénéficiaire à la demande du PSP du donneur d'ordre sera GRATUITE (pas d'interchange possible),
- La notification de la non correspondance sera quasi temps réel pour assurer une bonne fluidité du parcours client,
- En cas de défaillance du service (ou tout simplement si celui-ci n'est pas offert), la charge de la preuve de la fraude ou de l'erreur de saisie est portée par le PSP du donneur d'ordre, et le donneur d'ordre pourra exiger le remboursement de la totalité du virement sous 10 jours ouvrés même s'il avait autorisé l'opération,
- Le donneur d'ordre pourra se désinscrire s'il le souhaite (mécanisme « opt-out »).

AVIS du GT RED du FPF

Le service de vérification de la concordance entre l'IBAN et le nom du bénéficiaire représente une avancée majeure pour les clients particuliers et entreprises. Ce service est une première étape dans la lutte contre les fraudes aux virements autorisés, même s'il ne permettra pas de les éradiquer.

L'inversement de la charge de la preuve incitera les PSPs à mettre en place ce nouveau service.

Cependant la construction technologique de ce service reste à faire et c'est là que le "bât blesse" :

- Les règles et principes tels que proposés devront être précisés. Par exemple, il n'est pas défini à partir de quel seuil de concordance le PSP du donneur d'ordre doit notifier le donneur d'ordre. Ou encore le calcul du degré de concordance devra être homogène sous peine de mauvaise interprétation ; ce qui au final apportera de la confusion ou de la gêne au payeur qui serait notifié trop souvent à tort ;
- Les bénéficiaires entreprises devraient aussi pouvoir être identifiés grâce à leur identifiant (SIREN, LEI, numéro TVA intracommunautaire) en plus de leur nom, comme le propose aujourd'hui le service français SEPAm@il Diamond ;
- En laissant le marché s'organiser pour proposer une solution, il est probable que l'on assiste à plusieurs initiatives de place, susceptibles d'intervenir à différents moments de la chaîne du paiement (ex : au moment de l'initiation de l'ordre ou de sa compensation), ce qui posera à termes un problème d'interopérabilité entre ces différentes initiatives.

C'est pour ces raisons que le GT RED de France Payment Forum recommande :

- de mandater l'ERP et l'EPC sur la définition et l'évolution d'un *Scheme* avec des *Rulebooks* et des guides d'implémentation pour les messages d'échange en s'inspirant des solutions existantes telles que SEPAm@il Diamond ;
- de créer une marque et de communiquer globalement autour de cette marque ;
- de piloter et de suivre la mise en œuvre de ce nouveau service afin de corriger les éventuels problèmes ;
- de mettre en place ce service de manière progressive. Par exemple d'abord localement pour les particuliers, puis pour les entreprises puis en transfrontière.

5. Nécessaire objectivation des politiques du *de-risking*

Depuis l'entrée en vigueur de la DSP2, les PSP non bancaires (les *Third Party Providers* ou TPP) sont devenus plus nombreux et plus importants. Or pour offrir des services de paiement, ces acteurs (établissements de paiements, émetteurs de monnaie électronique, initiateurs de service de paiement) doivent avoir un compte auprès d'une banque commerciale pour les besoins du compte de cantonnement et pour l'accès aux infrastructures de paiement qui traitent et règlent les paiements.

La réalité du terrain montre que les banques opposent souvent des refus d'accès aux comptes bancaires commerciaux sans justification étayée ou accordent l'accès mais le retirent ensuite, la DSP2 ne leur imposant pas de s'expliquer sur leur appréhension de leurs propres risques.

Les PSP non bancaires sont donc dépendants des banques commerciales, non seulement pour le compte de cantonnement avec la protection des fonds des clients mais aussi pour l'exécution des paiements.

Rappelons la lettre de l'article 36 de la DSP2 (DIRECTIVE (UE) 2015/2366) qui traite de l'« Accès aux comptes détenus auprès d'un établissement de crédit » :

Les États membres veillent à ce que les établissements de paiement aient un accès objectif, non discriminatoire et proportionné aux services de comptes de paiement des établissements de crédit. Cet accès est suffisamment étendu pour permettre aux établissements de paiement de fournir des services de paiement de manière efficace et sans entraves. L'établissement de crédit communique à l'autorité compétente les raisons de tout refus.

Cet article 36 de la DSP2 a fait l'objet d'avis successifs :

- **En juin 2022**, l'EBA a émis un avis sur la réduction des risques (EBA/Op/2022/01).

L'EBA suggère que le caractère général de « l'article 36 de la PSD2 et le manque d'indications à l'intention des établissements de crédit sur les circonstances dans lesquelles la clôture d'un compte doit être notifiée ont donné lieu à une application divergente à travers l'UE et à des interprétations divergentes à travers les autorités de certification. »

- ❖ L'EBA recommande d'étendre le processus de notification de la phase d'intégration des PSP aux décisions prises par les établissements de crédit visant à exclure les établissements de paiement des relations commerciales existantes.
- ❖ Les normes techniques relatives aux processus de notification des refus pourraient faire l'objet d'un mandat confié à l'EBA afin de garantir l'application cohérente de l'article 36. Ainsi, lorsque les établissements de crédit décident de clôturer un compte, une formule selon un modèle obligatoire avec des explications circonstanciées devra être remonté aux

Position Paper PSR

Rédigé par : GT RED France Payments Forum

Auteurs : Marie-Laure Plessis, Alexandre Marion, Ludovic Vathelot et Corina Fontaine

Octobre 2023

autorités compétentes. Les régulateurs au niveau de l'UE pourraient obtenir des informations plus solides sur les raisons de clôture les plus courantes et prendre des mesures ciblées pour remédier à ces raisons.

- **Puis en février 2023**, l'étude « *Study on the application and impact of Directive (EU) 2015/2366 on Payment Services (PSD2) FISMA/2021/OP/0002* » est revenue sur les écueils du « *de-risking* ».

La réduction des risques, l'AML et les préoccupations RGPD sont au centre des refus subis par les PSP non bancaires (auprès des établissements de crédit qui indiquent que ces nouveaux acteurs présentent des cadres de contrôle et de conformité médiocres.

De l'autre côté, les EP/EME soutiennent que les banques utilisent trop souvent les dispositions sur la réduction des risques (*de-risking*) comme alibi pour restreindre l'accès aux comptes afin d'empêcher la concurrence. Des raisons « générales », faisant allusion à des risques inhérents vaguement définis, sont trop souvent invoquées dans le but, selon les EP/EME, de contrecarrer ou de restreindre l'innovation ou l'entrée sur le marché.

Bien qu'il existe des mesures destinées à garantir que l'accès soit proportionné et non discriminatoire, ce n'est pas le cas dans la pratique.

Les refus entraînent des interruptions du service des PSP non bancaires jusqu'à ce qu'une banque commerciale de remplacement soit trouvée et après un transfert de la connectivité de leur infrastructure vers la nouvelle banque commerciale. Par conséquent, il existe un risque de périodes sans aucun accès aux systèmes de paiement et sans capacité à protéger les fonds des clients, deux éléments essentiels pour que les PSP non bancaires puissent opérer leurs activités.

L'étude soutient l'avis de l'EBA qui proposait que lui soit donné mandat d'élaborer des normes techniques de réglementation afin de clarifier les interactions entre les exigences de LBC/FT et l'application de l'article 36 de la DSP2, limitant la réduction injustifiée des risques par les banques. En outre, l'idée est avancée que la Commission européenne pourrait envisager d'élargir cette exigence pour inclure également les décisions prises par les établissements de crédit de retirer les établissements de paiement des relations commerciales existantes.

- **Enfin en juin 2023**, la première mouture du PSR livre un ensemble de mesures sur le « *de-risking* »

On y trouve des mesures pour remédier aux défaillances et à rendre les règles de concurrence plus équitables :

- ❖ Exigence plus forte d'expliquer le refus, couvrant également, contrairement à la DSP2, le retrait du service :
 - Le participant à un système de paiement doit fournir à tout prestataire de services de paiement demandeur les raisons complètes d'une clôture de compte (par exemple une suspicion raisonnable d'activité illégale ou de risque pour l'établissement de crédit). Une raison générique ne suffit plus ;
 - le PSP peut faire appel aux autorités compétentes ;
 - L'EBA élabore des normes techniques de réglementation précisant le format harmonisé et les informations obligatoires dans la notification et la motivation.
- ❖ Les banques centrales seront autorisées à fournir des services de compte aux PSP non bancaires, à leur discrétion ;



Position Paper PSR

Rédigé par : GT RED France Payments Forum

Auteurs : Marie-Laure Plessis, Alexandre Marion, Ludovic Vathelot et Corina Fontaine

Octobre 2023

- La Commission propose également d'inclure les initiateurs de paiements parmi les participants possibles aux systèmes de paiement – avec des contrôles renforcés pour leur admission et une évaluation des risques appropriée.

En conclusion, les dispositions du règlement PSR suivent les recommandations de l'EBA et tiennent compte des alertes remontées en proposant des mesures ouvrant aussi des contournements aux accès via les banques commerciales, pour pouvoir opérer en dépit des refus dans la mesure où le PSP satisfait aux contrôles de risque. La volonté d'imposer un « *level playing field* » pour l'exercice de la concurrence en sortira renforcée.

AVIS du GT RED du FPF

Ces propositions visant à autoriser l'accès direct des TPP aux infrastructures de paiement ne sont pas sans poser des questions opérationnelles. À ce niveau de connexion, une résilience et des garanties de haut niveau sont indispensables.

Par ailleurs, les fortes restrictions de motifs de refus d'accès et les contraintes de déclaration de ces refus sont de nature à contrarier les banques commerciales, qui vont chercher une légitime compensation à cette quasi obligation de traiter avec des PSP qui concurrencent leur activité.

Le GT RED de France Payment Forum s'interroge sur l'efficacité de ces mesures pour dénouer les échanges et les crispations entre TPP et banques.