Document de position sur les projets de règlement (RSP) et de directive concernant les services de paiement et les services de monnaie électronique (DSP3)

France **FinTech** | novembre 2023

France FinTech

Document de position

sur les projets de règlement (RSP) et de directive (DSP3) concernant les services de paiement et les services de monnaie électronique

Novembre 2023

Introduction

Le **28 juin 2023**, la Commission européenne a présenté un **train de mesures visant à moderniser le cadre réglementaire applicable aux services financiers et au secteur des paiements pour l'adapter à la transformation numérique en cours**. Elle propose pour cela de **réviser l'actuelle directive sur les services de paiement (DSP2), qui deviendra la DSP3**, et d'établir, en outre, un **règlement sur les services de paiement (RSP)**. France FinTech et ses membres accueillent très favorablement ce paquet législatif présenté par la Commission européenne. **Ces nouvelles mesures sont, en effet, celles demandées par les fintech**, notamment en France, pour une meilleure mise en place des services financiers et de paiement innovants, **au service des citoyens et des entreprises**.

Avec la mise en œuvre de la **directive révisée sur les services de paiement (DSP2) en janvier 2018**, l'Union européenne (UE) a créé un cadre favorable au développement de nombreuses entreprises innovantes et de nouveaux services. Nous saluons également la **transition vers un cadre plus large que l'Open Banking avec l'Open Finance**, permettant l'accès à une gamme étendue de services financiers à un plus grand nombre de personnes. En élargissant le périmètre des données accessibles, elle ouvre la possibilité de fournir des **services plus personnalisés** et **adaptés aux besoins spécifiques des individus**, qu'il s'agisse de **micro-crédits**, d'**assurances abordables** ou de **solutions d'épargne adaptées**, qui sont autant de **nouvelles opportunités** pour les personnes qui, autrement, **auraient été exclues du système financier traditionnel**.

Pour assurer l'éclosion de ces innovations, il est important de **maintenir un accès aux données en temps réel** et d'**assurer le principe de parité** afin que les prestataires de services aient **accès aux mêmes données que le consommateur**. Il s'agit maintenant de **passer à l'échelle** pour **répondre aux besoins des consommateurs et des entreprises**, et **les propositions de DSP3 et de RSP représentent de formidables opportunités** pour l'écosystème des fintech. Aujourd'hui, **France FinTech et ses membres ont souhaité, à travers ce document de position, contribuer aux débats et proposer leurs remarques et suggestions pour faciliter la mise en œuvre future de ces initiatives**[1]. Celui-ci fait suite **à la diffusion par l'association en avril 2023 d'une position en amont de la publication des propositions législatives susmentionnées**.

Résumé de la position

L'**harmonisation réglementaire européenne en matière de paiements** en ligne est clé pour offrir aux prestataires de services de paiement **un cadre clair pour opérer dans le marché unique**. C'est la **condition nécessaire au développement de produits et services innovants** qui répondent au mieux aux **attentes et besoins des consommateurs**, tout en **renforçant la sécurité et la confiance dans les paiements électroniques.**.
Des **règles simples et directes** sont cruciales pour assurer une expérience utilisateur fluide et intuitive, en particulier lors de **l'interaction avec des solutions de paiement innovantes**. Les directives doivent faciliter plutôt qu'entraver l'utilisation des services par les consommateurs, en **évitant des étapes d'authentification répétitives et inutiles qui pourraient dissuader l'adoption de technologies émergentes**.

Pour **rester pertinente face à l'évolution rapide des technologies, la réglementation doit être flexible et "*futureproof*"**. En se concentrant sur des objectifs clairs tels que des **taux de fraude acceptables plutôt que sur des moyens spécifiques pour les atteindre**, la législation doit **encourager l'utilisation de technologies avancées et innovation pour**

[1] Compte tenu des calendriers envisagés, nous proposerons une contribution sur le projet de règlement relatif à un cadre pour l'accès aux données financières (*FIDA – Financial Data Access*) dans un second temps.

prévenir la fraude, tout en **soutenant l'émergence de méthodes de paiement novatrices et sécurisées**.

En résumé, ces trois éléments clés - harmonisation, simplicité et adaptabilité - sont essentiels pour créer un cadre réglementaire qui soutient la sécurité, l'efficacité et l'innovation dans le secteur des paiements en ligne.

Sommaire

Sur la nécessaire harmonisation et le RSP

La mise en place et l'application des règles de la DSP2 a conduit à des **incohérences entre certains des États membres de l'Union européenne**. **L'absence ou le manque de supervision dans quelques pays** a entraîné un **manque d'incitation pour certains acteurs traditionnels de respecter les règles de la directive** et cela a empêché le marché de fonctionner parfaitement. **Cette asymétrie de supervision a entraîné dans les faits une fragmentation du cadre réglementaire**. Le manque d'harmonisation des règles a **restreint le développement des fintech**, et les entreprises ayant des **modèles d'affaires paneuropéens** ont donc été **limitées dans leur expansion** au sein de l'Union européenne et au-delà.

Pour ces raisons, nous saluons **la mise en place de règles sous la forme d'un règlement - revêtant une portée générale, obligatoire dans tous ses éléments et directement applicable dans tous les États membres de l'UE** - sur les services de paiement à l'occasion de la révision de la DSP2. Nous accueillons également positivement le fait que le RSP introduit des **exigences pour les superviseurs nationaux (*National Competent Authorities - NCA*) d'appliquer les règles**, ainsi que des recommandations sur l'obligation pour les NCA d'avoir des **concertations avec les ASPSP (*Account Servicing Payment Service Providers*) ASPSP et TPP (*Third Party Providers*) afin de résoudre rapidement d'éventuels problèmes liés à l'accès ou le partage des données**.

Cet effort d'harmonisation des règles garantira une **application plus cohérente dans les États membres** de l'UE et **renforcera le rôle de la réglementation dans la promotion de l'innovation** et la **compétitivité en matière de paiement**. **Nous recommandons vivement que l'EBA (*European Banking Authority* - Autorité bancaire européenne) et les NCA intègrent explicitement les objectifs d'innovation et de compétitivité au sein de leur mandat**. En alignant leurs missions sur ces objectifs, ces institutions seraient mieux placées pour promouvoir un environnement financier robuste et agile.

Sur l'agrément et les licences (*article 45 de la DSP3*)

Nous saluons la proposition de la Commission d'harmoniser la réglementation de la monnaie électronique et des établissements de paiement, afin de simplifier son application. À l'issue d'une période de sauvegarde, les établissements de monnaie électronique qui relevaient auparavant de la deuxième directive sur la monnaie électronique devront obtenir un nouvel agrément en vertu de la DSP3. **Ce processus devrait être simplifié et rationalisé dans tous les États membres** afin de permettre une transition en douceur, de s'assurer de règles du jeu identiques dans toute l'Union européenne et de limiter la charge supplémentaire pour le secteur et les autorités compétentes. Ainsi, les établissements bénéficiant de droits acquis ne devraient être tenus de satisfaire qu'aux nouvelles exigences de la DSP3 en matière d'agrément et ne devraient pas avoir à soumettre à nouveau les informations fournies dans le cadre du (ré)agrément au titre des DSP2 et EMD2 (*Second Electronic Money Directive*), qui font actuellement l'objet d'une surveillance.

Sur les définitions (*article 2 de la DSP3*)

Nous saluons les clarifications apportées par le projet de DSP3 sur le champ d'application et les définitions. **La définition des "agents" pourrait être davantage clarifiée et harmonisée entre les États membres** afin de **refléter l'évolution des réalités du marché**. Il convient de rappeler que les places de marché et les plateformes soutenues par les prestataires de services de paiement qui leur retirent le contrôle des fonds pour des tiers, ne sont pas par défaut des agents du prestataire de services de paiement.

Sur l'accès aux systèmes de paiement (*article 31 du RSP, article 46 de la DSP3*)

L'impossibilité pour les établissements non bancaires et les petits établissements de crédit d'accéder à l'infrastructure des banques centrales sur une base non discriminatoire **crée des conditions de concurrence inégales entre les différents types d'établissements**

réglementés. Demain, l'accès direct aux systèmes de paiement ne permettra pas seulement de **réduire une distorsion de la concurrence** et un meilleur accès à l'innovation, cela **ouvrira également la possibilité à des petits établissements, jusqu'ici écartés, d'adhérer aux systèmes de paiement via de nouveaux partenaires**. Ce sera alors un cercle vertueux, améliorant à la fois la **solidité de notre système de paiement** et répondant à l'important **défi de la souveraineté numérique**. Cela permettra également l'émergence **d'acteurs innovants de plus grande envergure capables de rivaliser avec leurs concurrents sur la scène internationale**.

Il sera cependant essentiel de préparer les conditions nécessaires pour garantir l'efficacité de la mesure et de sa mise en œuvre. La révision de la directive sur la finalité des règlements (*Settlement Finality Directive* - SFD) devrait s'accompagner d'une mise à jour des systèmes utilisés par les banques centrales. Cette mise à jour est nécessaire pour que, dans les faits, les nouveaux arrivants puissent accéder aux systèmes de paiement comme TIPS (*Target Instant Payment Settlement*) et Target2 (*Trans-European Automated Real-time Gross Settlement Express Transfer System*).

L'interopérabilité des systèmes de paiement au sein de l'UE, ainsi que les règles d'accessibilité, seront les principaux défis de la réforme. À cet égard, nous tenons également à souligner **l'importance de l'interopérabilité entre l'Open Banking et l'Open Finance**, élément clé pour assurer des **parcours clients efficaces**. Pour que l'expérience utilisateur soit fluide et sans heurts, il est primordial que les AISP (*Account Information Service Providers*) puissent accéder, via une interface unique, à tout type de compte - qu'il soit de paiement, comme prévu par DSP3/RSP, ou non-paiement, comme envisagé dans le cadre de la FIDA (règlement *Financial Data Access*). Une telle harmonisation garantirait une expérience client uniforme, répondant aux attentes des consommateurs européens modernes.

Sur le cadre de l'Open Banking (*articles 35-39 et 89 du RSP*)

L'évolution du paysage financier en Europe a été considérablement influencée par les initiatives d'Open Banking. Bien que le RSP n'introduise pas de nouveautés radicales, **il apporte une précision bienvenue, rappelant les principes fondamentaux de l'Open Banking** tout en **fournissant une description plus détaillée et claire de ces principes**.

L'accès aux données, soutenu par les infrastructures de paiement instantané, fournit une base solide pour des paiements plus innovants, plus sûrs et plus compétitifs en Europe. Cependant, **il était nécessaire de clarifier le cadre réglementaire**, comme la Commission européenne l'a fait avec le projet de règlement. Les **banques ont besoin de clarté sur ce qu'on attend d'elles** et **d'incitations à investir afin de garantir la fourniture de services de qualité**. Cela représente une formidable opportunité pour l'innovation par les prestataires de services de paiement. **Il existe aujourd'hui un large éventail d'initiatives différentes et la fiabilité des API (Application Programming Interface) bancaires est inégale**. L'article 38 indique des mesures de contingence pour les situations où les interfaces (API) sont indisponibles. Toutefois, il est crucial de comprendre qu'**au-delà de la simple indisponibilité, d'autres problèmes tels que l'absence de certaines fonctionnalités (ex. possibilité de récupérer certaines données essentielles), une expérience client médiocre, l'instabilité ou des temps de réponse prolongés peuvent survenir**. Il est regrettable que **les mesures de contingence pour de tels cas ne soient pas explicitement mentionnées dans le texte**.

Cela **entrave la capacité des prestataires de services de paiement à développer des solutions pour intégrer les API**. Nous soutenons fermement l'**inclusion des notions de performance et d'obstacle dans le texte**, car elles sont d'une importance cruciale. **Leur absence limite non seulement le développement de fonctionnalités intéressantes grâce à l'Open Banking, mais met également en péril l'efficacité de l'ensemble de l'écosystème fintech**.

Les paiements récurrents en sont un exemple : les consommateurs d'aujourd'hui paient des entreprises qui disposent d'une gamme de nouveaux modèles commerciaux - y compris des services à la demande et par abonnement. Les paiements récurrents de l'Open Banking pourraient considérablement élargir l'ensemble des solutions de paiement disponibles pour soutenir ces modèles commerciaux.

Il pourrait être intéressant que la Commission **adopte des objectifs de niveaux de services/de fiabilité plus stricts pour les interfaces des ASPSP**, ainsi que **des sanctions appropriées contre les ASPSP qui ne les respectent pas**, et **que soit spécifié un socle minimal d'informations pouvant être récupérées par les AISP** :

- Trois (3) mois d'historique bancaire ;
- Et les informations permettant de confirmer l'identité de l'utilisateur (nom et prénom, date et lieu de naissance, etc.) : ces informations devraient être ajoutées au 2.d de l'article 36, qui devrait également concerner les AISP (et pas uniquement les PISP - prestataires de services d'initiation de paiement - comme c'est le cas dans le projet de règlement proposé par la Commission européenne).

Il conviendrait fortement d'**encourager, voire de mandater, les ASPSP à adopter des solutions basées sur la communication *app-to-app*, afin d'optimiser la fluidité des parcours utilisateurs**. Cette approche, déjà mise en œuvre avec succès au Royaume-Uni, s'avère efficace, comme en témoignent les lignes directrices sur le sujet.

Sur les exemptions à l'authentification forte et la responsabilité (*articles 60, 85 et 86 du RSP*)

L'Union européenne a joué un rôle de premier plan dans la réduction de la fraude dans les paiements en ligne, l'authentification forte du client (Strong Customer Authentification, SCA) devenant la norme dans de nombreuses juridictions en dehors d'Europe. Cependant, nous observons que **certains acteurs continuent à décourager les utilisateurs de faire usage des services proposés par les TPP en les obligeant à passer par plusieurs SCA** sur leurs

interfaces dédiées. Ces multiples demandes ajoutent aux frictions dans le parcours client une expérience plus pauvre, et surtout n'ajoute pas à la sécurité. Tout cela **réduit l'innovation que peuvent apporter les nouveaux acteurs, et le choix pour les consommateurs**. Nous appelons la Commission à une **approche "technologie-neutre" et "risk-based" en ce qui concerne les règles de SCA**.

Ces dernières années, **le secteur - les commerçants, les acquéreurs, les réseaux de cartes et les émetteurs - a collectivement réalisé des investissements importants pour adopter l'authentification à deux facteurs et les protocoles de messagerie 3DS2** pour affiner le parcours de SCA des consommateurs européens. Une **clarification de la responsabilité du prestataire de services de paiement du bénéficiaire pourrait permettre de rationaliser davantage l'acceptation de ces exemptions dans l'ensemble du secteur**.

Sur la flexibilité technologique en matière d'authentification forte (*articles 83, 85 et 89 du RSP*)

Bien que l'authentification forte ait contribué à réduire la fraude dans les paiements en ligne, **les dispositions actuelles définissent de manière prescriptive la solution technologique requise** : l'authentification à deux facteurs. Or, dans certains cas, il est impossible de l'appliquer. En parallèle, les fraudeurs trouvent tous les jours des moyens toujours plus innovants de contourner les règles. Les anciennes méthodes de lutte contre la fraude n'ont pas été conçues pour les pratiques actuelles en ligne et peuvent conduire à des taux d'acceptation plus faibles et à des pertes de revenus. Au lieu de cela, la technologie et l'innovation devraient jouer un rôle pour mieux comprendre le client et détecter la fraude. **Une réglementation basée sur les résultats - fixant des exigences en matière de taux de fraude sans définir les outils utilisés pour y parvenir - permettrait de garantir que la technologie et l'innovation soient mises à profit dans la lutte contre la fraude aux paiements en ligne**.

Sur les autres outils de prévention de la fraude (*articles 3, 50, 62, 83 et 84 du RSP*)

Si l'authentification forte peut contribuer à réduire la fraude, il ne peut s'agir d'une solution unique en matière de protection contre la fraude. Les prestataires de services de paiement emploient déjà aujourd'hui toute une série d'outils différents pour détecter et atténuer le risque de fraude. Il conviendrait de **s'assurer que les utilisateurs des services de paiement soient conscients des différents types de fraude et de la manière de les identifier**.

Sur la nécessité et l'autorisation de collaborer entre acteurs régulés en matière de lutte contre la fraude (*article 80 et 83 RSP*)

L'ensemble des acteurs régulés (banques, établissement de paiements, etc.) doivent disposer d'un cadre juridique les autorisant à s'échanger en toute sécurité des informations en cas de soupçon de fraude. Actuellement, **certains textes** (secret bancaire, secret professionnel, RGPD, etc.) **rendent complexe la possibilité d'échanges d'information** entre les acteurs régulés. Nous saluons donc l'initiative de la Commission européenne visant à **mettre en place un cadre permettant d'envisager un partage d'informations relatives à la fraude entre PSP**.

Il nous semble toutefois que **les cas susceptibles de donner lieu à de tels échanges qui sont prévus dans le projet de règlement (article 83.3) sont trop restrictifs**. En effet, devraient pouvoir faire l'objet d'échanges **les informations relatives aux fraudeurs ayant fait l'objet de signalement, soit par d'autres clients du PSP**, soit par d'autres PSP. Il semblerait d'autre part souhaitable que **le périmètre des informations pouvant être partagées ne se limite pas aux seuls identifiants uniques, mais couvre plus largement les informations relatives à ces fraudeurs et permettant de les identifier** y compris lorsqu'ils utilisent des coordonnées bancaires différentes. Nous souhaitons que **des outils de lutte contre la fraude puissent être labellisés** pour faciliter le partage d'informations relatives à la fraude entre PSP, en architecture de base de données distribuées.

Autres mesures susceptibles d'être introduites dans le RSP

Un certain nombre d'autres mesures, ou de précisions, pourraient utilement être prévues dans le règlement sur les services de paiement :

- Prévoir **l'obligation pour les systèmes de paiement de mettre en place des dispositifs exhaustifs et automatisés permettant la contestation et la représentation par les parties prenantes d'une transaction**, en vue de limiter la fraude tout en protégeant chaque partie.
- Mieux clarifier le fait qu'**une authentification forte n'est nécessaire, dans le cas d'une série de transaction, que lors de la première transaction**. Et donc, que le *liability shift* **a aussi vocation à s'appliquer aux transactions ultérieures**. En effet, actuellement les banques émettrices et certains PSP considèrent, à tort, que dans le cas d'une série de transactions le 3DS réalisé lors de la première transaction ne couvre que cette dernière - et approuvent donc (au motif de l'absence de 3DS) des *chargebacks*, relatifs aux transactions ultérieures de la même série, qui devraient être refusés.
- Prévoir une dérogation à l'article 49.7 : **les utilisateurs de services de paiement devraient avoir la possibilité**, dans certains cas bien encadrés (e.g. achat d'un bien/service en plusieurs fois), **de renoncer à leur droit de mettre fin à tout moment à une autorisation d'exécuter une série de transactions**.
- Imposer la f**ixation de plafonds aux frais applicables en cas d'échec de la réalisation d'un service de paiement** - et notamment de débit SEPA initié par le bénéficiaire.

À propos de France FinTech

Créée en juin 2015 à l'initiative des entrepreneurs, France FinTech est une association à but non lucratif dont la mission est de promouvoir l'excellence du secteur en France et à l'étranger et de représenter les fintech françaises auprès des pouvoirs publics, des régulateurs et de l'écosystème. Elle rassemble les fintech, assurtech et regtech françaises ayant le potentiel de devenir des leaders européens ou mondiaux. Autour des start-up se sont réunis tous les acteurs souhaitant accompagner ce mouvement et se faire reconnaître comme partie intégrante de l'écosystème : sociétés technologiques, fonds d'investissement, cabinets d'avocats et de conseil, banques, assureurs, entreprises industrielles, entités publiques ou associatives, etc.

Contacts

Alain Clot
Président
alain.clot@francefintech.org

Kristen Charvin
Déléguée générale
kristen.charvin@francefintech.org