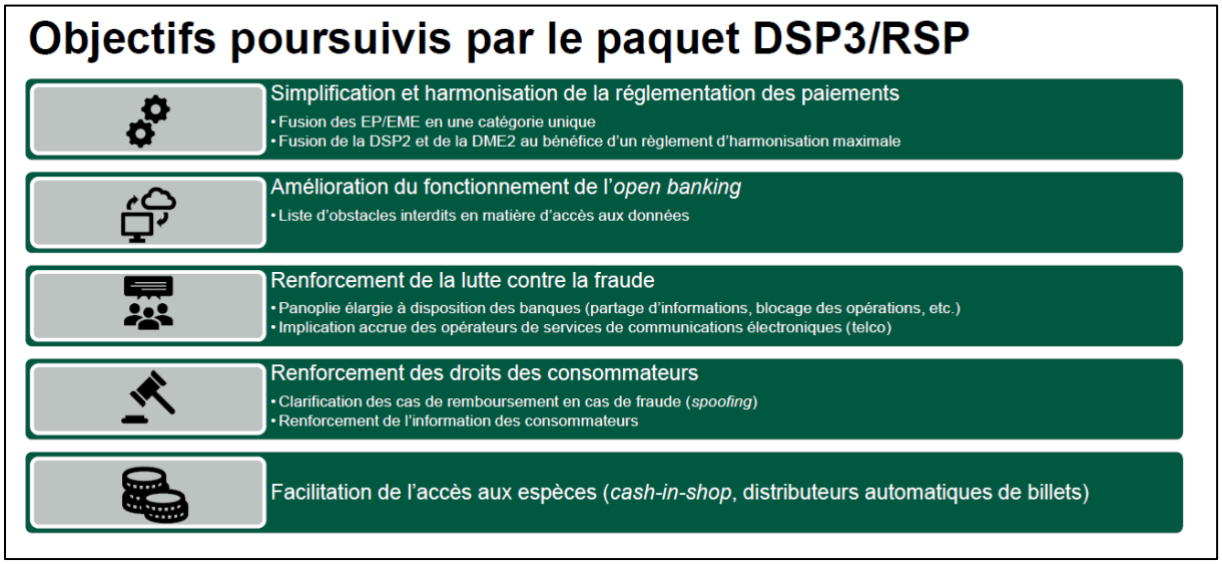
FRANCE PAYMENTS FORUM

Plénière mensuelle du 21 mai 2026

David Sabban (Direction générale du Trésor)

Le point sur le paquet « paiements » (DSP3/RSP)

Objectifs et calendrier du paquet « paiements »



Simplification et harmonisation de la réglementation des paiements

On fusionne la DSP2 et la DME2 pour en faire un règlement et une directive : le règlement fixe les obligations applicables aux acteurs ; la directive fixe les modalités d'agrément et de supervision. L'objectif est d'avoir des textes d'harmonisation maximale pour favoriser le *level-playing-field* et éviter des comportements potentiellement opportunistes.

Amélioration du fonctionnement de l'open banking

À l'heure où on parle de souveraineté des moyens de paiement, certains acteurs oublient de parler de l'open banking, alors que c'est un moyen de paiement souverain et pan-européen.

Renforcement de la lutte contre la fraude

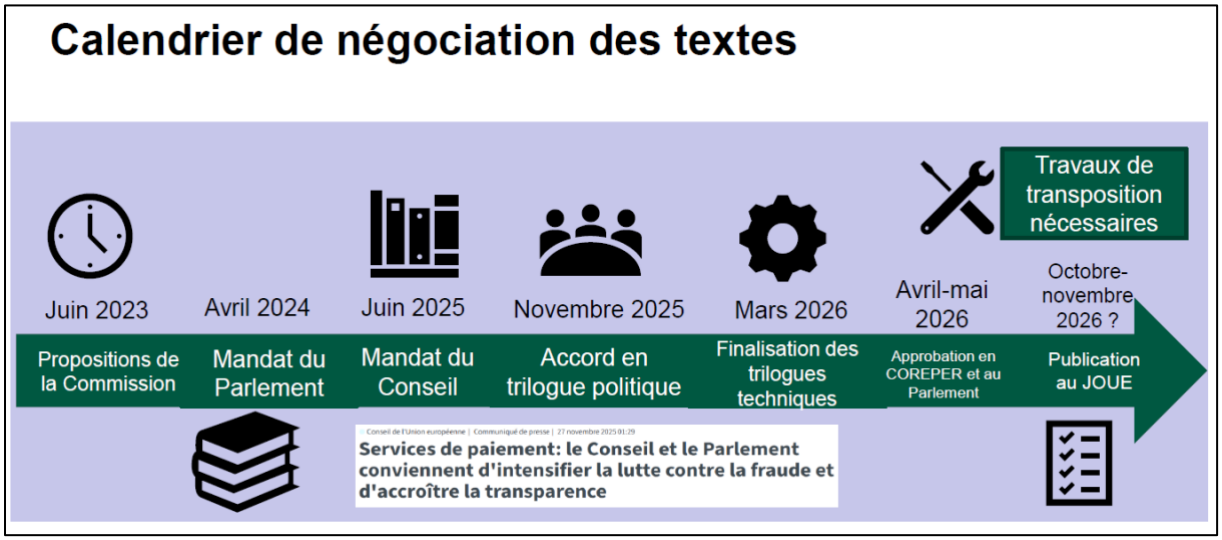
Le renforcement de la lutte contre la fraude est évidemment le point qui suscite le plus d'attention politique, et sur lequel la France a particulièrement pesé dans le cadre des négociations. Le paquet « paiements » va substantiellement renforcer la panoplie à disposition des prestataires de services de paiement (PSP).

Renforcement des droits des consommateurs

Autre point important, qui a notamment retenu l'attention du Parlement européen : les droits des consommateurs, en matière de remboursement en cas de fraude et en matière d'information.

Facilitation de l'accès aux espèces

Lorsque la Commission européenne a publié fin juin 2023 son paquet « Single Currency », outre les deux textes sur l'euro numérique, il y avait également un texte sur le cours légal des espèces. Le discours très clair des institutions européennes (et de la France) est que l'euro numérique ne remplace pas les pièces et les billets mais vient en complément, pour élargir la panoplie de choix des utilisateurs. L'accès aux espèces est un sujet d'une très grande sensibilité (à la DGT, nous le voyons notamment à travers des amendements, des questions écrites au gouvernement, des interpellations…) et la Banque de France est à juste titre très mobilisée sur le sujet.



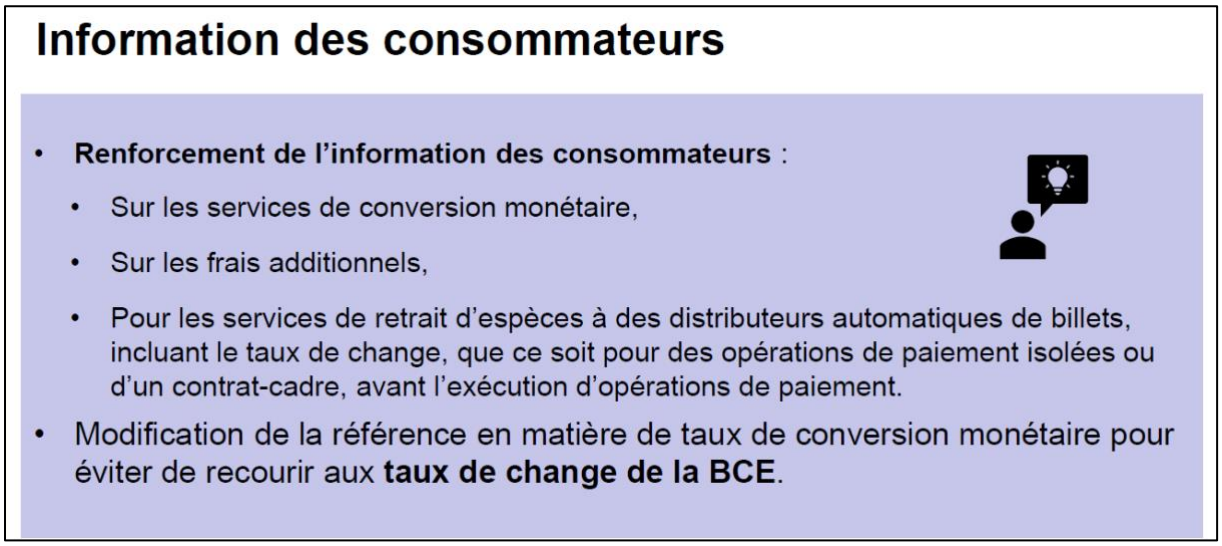
Comme je le rappelais plus haut, les propositions de la Commission européenne pour la DSP3 et le RSP ont été publiés fin juin 2023. Le Parlement européen a adopté son mandat en avril 2024, juste avant les élections européennes de 2024, et ce n'est pas sans conséquences, car le Parlement a dû aller assez vite pour finaliser son mandat afin de ne pas devoir tout reprendre à zéro dans le cadre de la nouvelle législature.

Du côté du Conseil, on s'est mis d'accord en juin 2025 (sous présidence polonaise), et on a eu un accord en trilogue politique en novembre 2025 (sous présidence danoise). Mais l'accord en trilogue politique est juste un « accord » sur les grandes lignes entre le Parlement européen, la Commission et le Conseil, qu'il faut ensuite traduire dans le détail, disposition par

disposition, considérant par considérant, dans le cadre de « trilogues techniques ». Ceux-ci se sont achevées fin mars 2026. Les textes ont été approuvés en COREPER (Comité des représentants permanents des gouvernements des États membres de l'Union européenne) le 5 mai. Les prochaines étapes sont l'adoption formelle par le Parlement européen en séance plénière, et la traduction des textes.

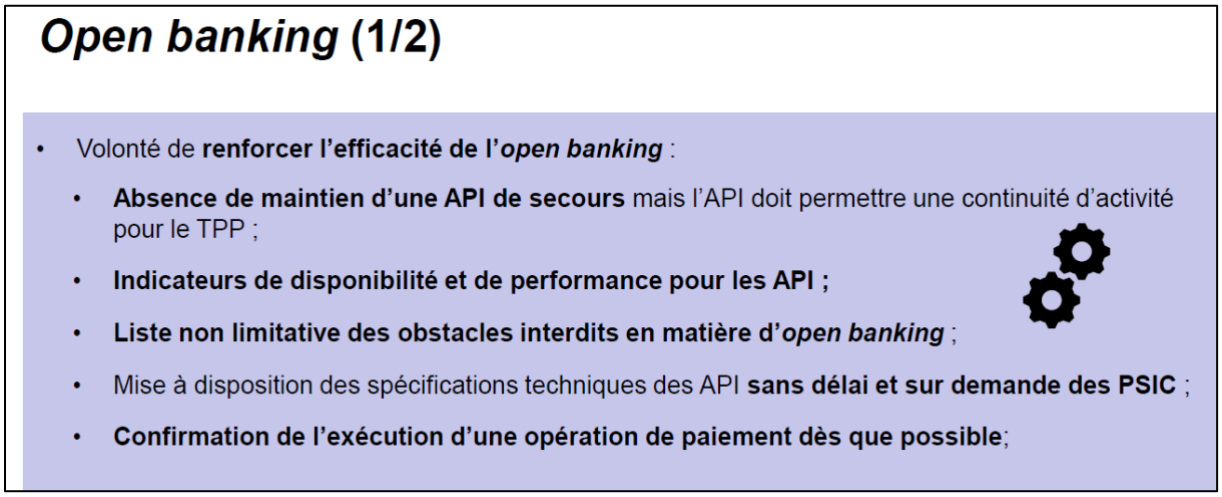
Les textes sont négociés en anglais (langue de travail), mais sont ensuite traduits dans toutes les langues de l'Union européenne, et toutes les traductions linguistiques ont la même valeur juridique. C'est un point un peu méconnu du public, mais cette étape de traduction est essentielle car les textes ainsi traduits ont vocation à s'intégrer dans les différents droits nationaux. C'est donc une étape qui prend un peu de temps, et c'est pourquoi j'ai mis un point d'interrogation concernant la date de publication des textes au Journal Officiel de l'Union européenne (octobre-novembre 2026 ?). Cette date-là est importante parce qu'elle détermine la date d'entrée en vigueur des textes, la date de transposition de la DSP3 et la date d'entrée en application du RSP, 21 mois après la date d'entrée en vigueur, c'est-à-dire *a priori* mi-2028.

En droit français, ces textes vont impacter un certain nombre de codes : le code monétaire et financier, le code de la consommation, le code des postes et des communications électroniques… Nous avons donc devant nous des travaux assez denses. La voie traditionnelle de transposition est de passer par ordonnances, ce qui suppose une habilitation du Parlement pour légiférer par ordonnance.



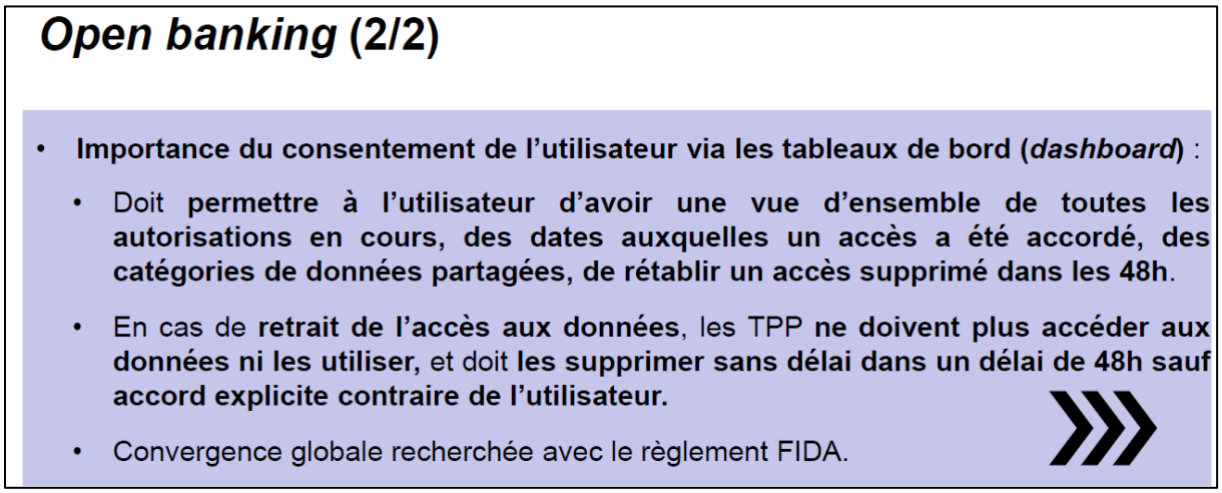
Le renforcement de l'information des consommateurs porte sur les frais de paiement et sur ce qu'on appelle les « services de conversion monétaire » (quand vous faites un virement qui implique une conversion dans une autre devise). Il porte également sur les services de retrait d'espèces. L'idée, qui fait largement consensus, est de renforcer l'information du

consommateurs afin que celui-sache, avant d'effectuer un paiement (ou un retrait), la décomposition exacte des frais qu'il aura à payer.



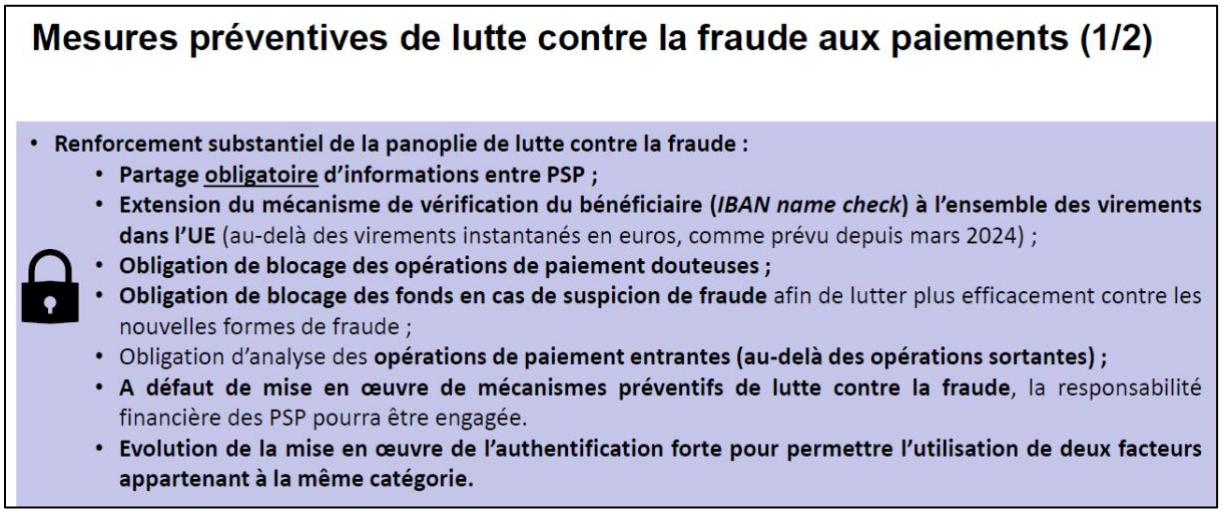
L'open banking étant insuffisamment déployé en comparaison d'autres juridictions (notamment le Royaume-Uni), l'idée est de renforcer son efficacité en levant certains obstacles qui se traduisent par des échecs techniques en matière, par exemple, de redirection, d'authentification forte, afin de donner à l'open banking son plein potentiel à l'utilisation.

L'idée est aussi de simplifier les API de secours (les « *fallback interfaces* ») : dès lors que l'on fait de l'open banking, il faut que les API déployées par les banques aient un niveau extrêmement élevé de performance, d'efficacité et de disponibilité.



Autre point important : le consentement de l'utilisateur. Dès lors qu'un utilisateur donne accès à ses données de paiement, il faut lui permettre de savoir à qui il a donné accès à ses données de paiement et s'il peut retirer l'accès. L'objectif est donc de permettre à l'utilisateur d'avoir des tableaux de bord (*dashboards)* lui donnant une vue d'ensemble sur les autorisations qu'il a données en matière d'accès à ses données de paiement. L'idée globale, du côté des co-législateurs, est de rechercher une convergence avec le règlement FIDA (qui porte sur les

données financières hors données de paiement), pour d'avoir *in fine* une cohérence entre ces deux textes qui permettent l'accès aux données financières, au sens large



Au cœur du règlement sur les services de paiement (RSP) il y a la prévention de la fraude au paiement.

Partage d'informations entre PSP

Le partage obligatoire entre PSP d'informations sur la fraude est un point sur lequel la France a pesé fortement dans la négociation. Comme Hervé Sitruk l'a rappelé dans son propos introductif, en France les arrêtés relatifs au fichier national des comptes signalés pour risque de fraude (FNC-RF) ont été publiés fin avril (arrêté technique et arrêté tarifaire) et le FNC-RF est opérationnel depuis le 7 mai. Le FNC-RF préfigure ce partage au niveau européen. C'est à la fois une architecture technique et un dispositif réglementaire. Le FNC-RF a vocation à s'interfacer avec ce qui sera construit au niveau européen. Les discussions sont en cours avec l'EPC en matière de standards.

Quand on parle de partage d'informations entre PSP, il y a évidemment une attention très forte en matière de données personnelles. Ce sont des questions très sensibles, comme l'a souligné la CNIL dans son avis sur le FNC-RF.

Extension de la VoP à l'ensemble des virements dans l'Union européenne

Au-delà des virements instantanés en euros tel que prévu par le règlement de mars 2024 entré en application le 9 octobre 2025.

Obligation de bloquer les opérations de paiement douteuses

Les PSP doivent bloquer les fonds entrants en cas de suspicion de fraude, c'est-à-dire faire du « transaction monitoring » non seulement sur les paiements sortants mais aussi sur les

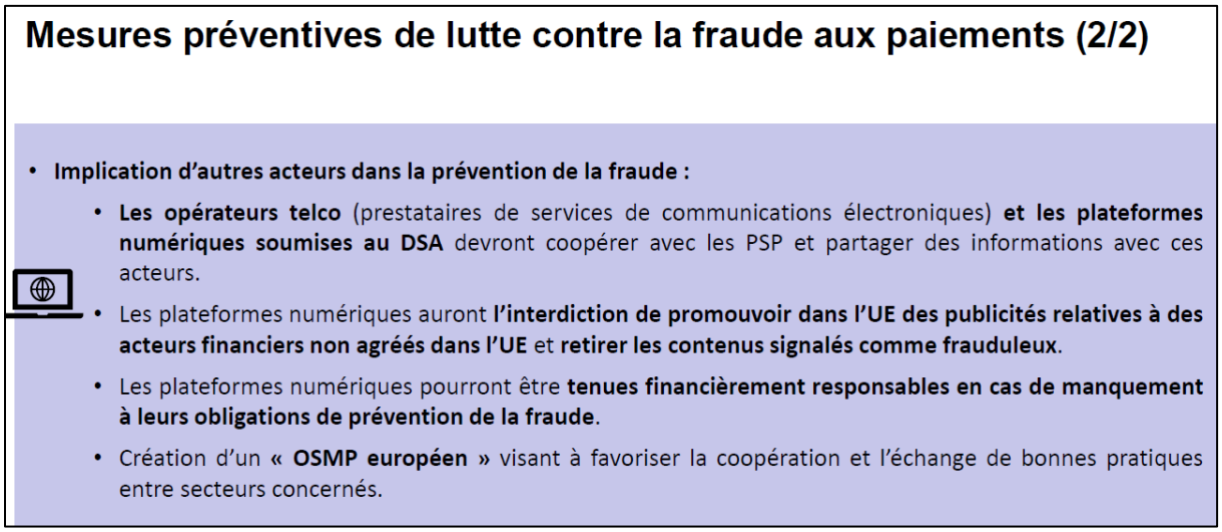
paiements entrants. L'idée est de lutter plus efficacement contre ce qu'on appelle les « comptes-rebonds » auxquels l'ACPR a récemment consacré une note très claire[1].

Responsabilité des PSP

Le RSP prévoit également que si les PSP ne mettent pas en œuvre les mécanismes préventifs de lutte contre la fraude et qu'il s'ensuit un préjudice pour l'utilisateur, la responsabilité financière des PSP pourra être engagée.

Évolution de la mise en œuvre de l'authentification forte

Il y avait une attention forte de la Commission et du Parlement pour adapter l'authentification forte aux nouvelles modalités d'initiation des paiements. Il a donc été prévu que l'on pourrait faire évoluer la mise en œuvre de l'authentification forte pour permettre l'utilisation de deux facteurs appartenant à la même catégorie, à partir du moment où leur indépendance et leur robustesse sont maintenues. Les autorités françaises, notamment la Banque de France qui est en charge de la surveillance des paiements, seront très attentives à ce que cette adaptation n'affaiblisse pas le dispositif global de l'authentification forte issu de la DSP2 et qui a très largement fait ses preuves en termes de sécurité des paiements.



Implication des acteurs telco et des plateformes numériques

Quand on parle de fraud aujourd'hui, dans un contexte d'industrialisation de la fraude, on ne peut plus se limiter aux PSP, il faut penser plus large et inclure dans le paysage les opérateurs telco. On voit se multiplier les arnaques au faux conseiller bancaire et, plus largement, les fraudes par manipulation.

[1] Rapport sur la prévention des comptes rebonds pour le blanchiment d'escroqueries et autres fraudes | Autorité de contrôle prudentiel et de résolution (juillet 2025)

Il faut également inclure les plateformes numériques, donc les hébergeurs, les moteurs de recherche en ligne, les acteurs soumis au DSA. L'idée est d'obliger ces acteurs à avoir des canaux d'échange, protéger leurs informations, et, dans le respect de leurs obligations légales, contribuer et prévenir la lutte contre la fraude. Par exemple, cela concerne la typologie de fraude dans laquelle un fraudeur va prendre le contrôle d'une ligne téléphonique afin de tenir en échec les mécanismes d'authentification forte qui reposent souvent sur la ligne téléphonique.

Réglementation de la publicité des plateformes numériques

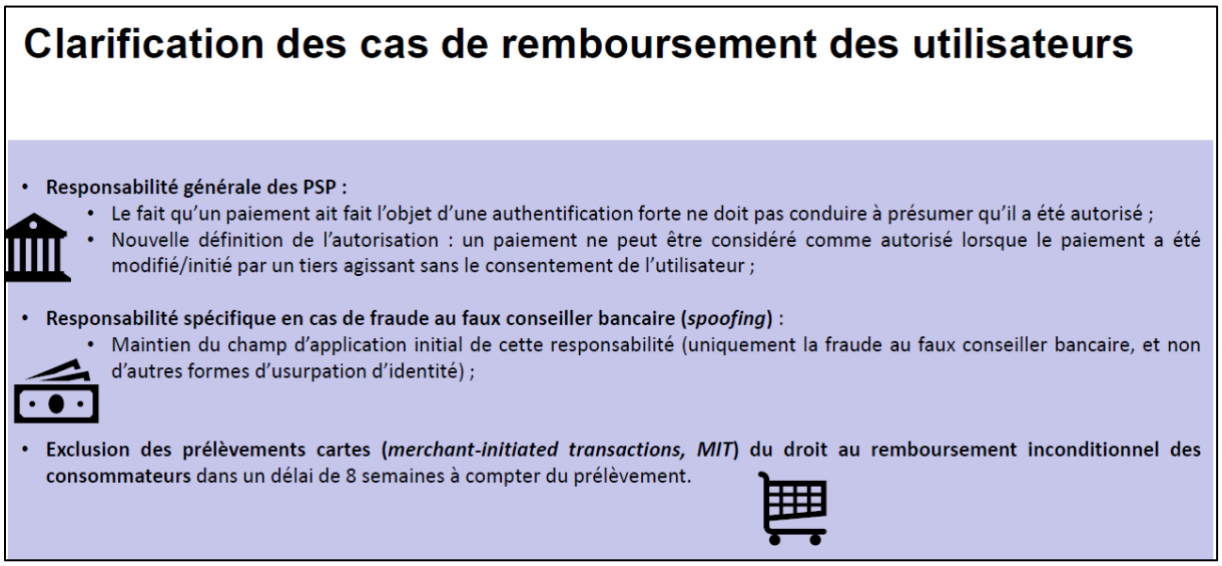
Le texte prévoit explicitement que les plateformes numériques ne pourront pas faire de la publicité dans l'Union européenne pour les acteurs financiers qui ne sont pas agréés. L'idée est vraiment de stopper la diffusion de toute publicité frauduleuse dans l'UE.

Responsabilité des plateformes numériques

Le texte prévoit également que si les plateformes numériques manquent à leurs obligations en matière de prévention de la fraude et qu'il en résulte un préjudice, les PSP, pourront se retourner contre elles.

Création d'un OSMP européen

Cet équivalent européen de l'OSMP est appelé « plateforme européenne de lutte contre la fraude ». L'idée est de rassembler les autorités publiques, le secteur privé (PSP, telcos, plateformes numériques, prestataires techniques…) pour faciliter la coopération, l'échange de bonnes pratiques entre ces différents acteurs.



Responsabilité générale des PSP en matière de paiement non autorisé

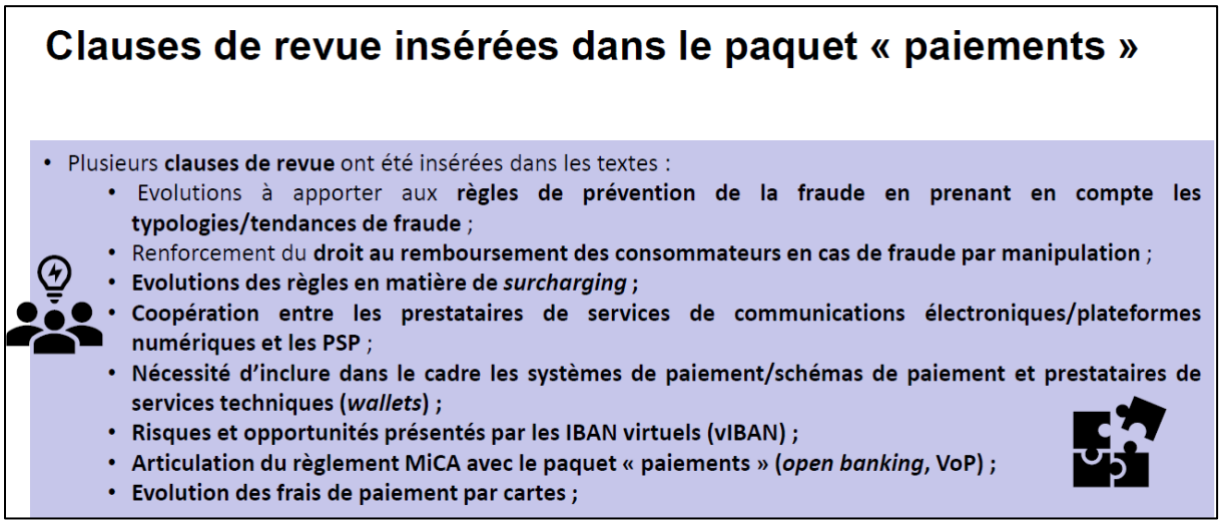
Les textes apportent deux ajouts importants en la matière.

- Le fait qu'un paiement ait fait l'objet d'une authentification forte ne doit pas toujours conduire à présumer que l'opération a été autorisée. Ceci renvoie aux recommandations de l'OSMP de mai 2023 sur les modalités de remboursement des opérations de paiement frauduleuses. C'est un point sur lequel la France a beaucoup insisté et sur lequel il y a eu un large au Conseil et au Parlement. Les banques ne peuvent pas dire que dès lors qu'un paiement a fait l'objet d'une authentification forte, il est considéré comme autorisé.

  Le RSP donne une nouvelle définition de l'autorisation : un paiement ne peut pas être considéré comme autorisé lorsqu'il a été modifié ou initié par un tiers sans le consentement de l'utilisateur. Autrement dit, un paiement ne peut pas s'effectuer sans le consentement de l'utilisateur, même s'il n'est pas toujours initié par celui-ci.

- Le RSP introduit une responsabilité spécifique en cas de fraude au faux conseille bancaire (*spoofing*). Il faut savoir que le Parlement européen souhaitait que pour toute fraude liée à l'usurpation d'identité de n'importe quelle entité, publique ou privée (faux agent des impôts, faux agent municipal, faux représentant d'une association ou d'une entreprise…), la banque puisse être tenue pour responsable. Un tel élargissement n'a pas été jugé admissible du côté du Conseil. Le texte, désormais stabilisé, maintient donc que cette responsabilité de la banque ne vaut qu'en cas de fraude au faux conseiller bancaire.

Évolutions à venir ?



Le paquet « paiements » prévoit un certain nombre de clauses de revue sur des points sur lesquels les négociateurs ont estimé qu'il serait prématuré de légiférer ou qu'il fallait se laisser un peu de temps pour voir comment le marché évolue, l'idée étant de rester en agilité et en alerte.

- Des rapports seront demandés à la Commission notamment en matière de surcharging. Sur ce point, les textes ne changent pas fondamentalement ce qui figurait déjà dans la DSP2 : le Parlement européen voulait interdire le surcharging, mais c'est un point sur lequel le Conseil a tenu bon, considérant qu'on ne peut pas totalement interdire le surcharging.
- Des réflexions sont à venir sur la coopération entre PSP et opérateurs telco et plateformes numériques.
- Une réflexion est aussi à venir sur l'inclusion dans le cadre des systèmes de paiement, des prestataire techniques et wallets. Ces acteurs ne sont pas inclus dans le périmètre de la réglementation européenne car ils sont considérés comme des acteurs techniques, support, mais il faudra se poser la question : quelle réglementation, quelle supervision, quelles obligations ? Faut-il aller plus loin que ce qui est prévu dans le PISA Framework de l'Eurosystème ?
- Autre point important, sur lequel la France a beaucoup œuvré : une transparence accrue en matière de frais de paiement par carte. Les commerçants se plaignent beaucoup auprès des politiques là-dessus. Des rapports seront demandés à la Commission européenne pour mesurer l'évolution des frais de paiement par carte par un certain nombre d'acteurs et évaluer la capacité des acquéreurs, des émetteurs et finalement des marchands, parce que ce sont eux qui payent les frais, en matière de frais de paiement par carte.

Merci de votre attention

****

Hervé Sitruk

Merci David.

Cela fait maintenant 25 ans qu'on légifère au niveau européen et on a toujours une forte fragmentation. Faut-il considérer que c'est inexorable car c'est la réalité du marché ou car il y a des gens qui ne veulent pas jouer le jeu, ou bien que la réglementation n'est pas adaptée ? Avec ce règlement sur les services de paiement, va-t-on enfin sortir de cette problématique de la fragmentation ?

David Sabban

L'harmonisation réglementaire est une condition nécessaire pour réduire la fragmentation, mais pas une condition suffisante. Il est évident que si nous sommes passés d'une directive à un règlement (choix contesté par certains États membres au début des négociations), c'est pour avoir une harmonisation maximale, notamment en matière de remboursement des utilisateurs en cas de fraude au paiement.

Nous avons beaucoup œuvré pour clarifier un certain nombre de notions dans les textes : par exemple, la notion d'agent de prestataire de services de paiement. C'est un sujet sur lequel nous avons eu beaucoup de discussions avec nos partenaires européens et l'Autorité bancaire européenne. Tout ce qui est relatif aux passeports (les passeports triangulaires) ou aux pratique de supervision, est pour nous très important.

Nous avons ce débat-là dans tous les textes : par exemple en matière de cryptoactifs, la France pousse pour que la supervision des prestataires de services sur cryptoactifs remonte au niveau de l'ESMA. L'harmonisation réglementaire est donc une brique nécessaire, mais pour mettre fin à la fragmentation des marchés, il faut beaucoup d'autres choses.

Le rôle des autorités européennes est extrêmement important. Par exemple, on a parlé il y a quelques années des IBAN virtuels : c'est un sujet qu'on voit monter de plus en plus, qui offre des possibilités très utiles en matière de réconciliation des paiements, de cash-pooling… mais qui peut aussi créer de nouveaux risques. Il faut trouver un équilibre entre harmonisation réglementaire et déploiement de l'innovation. Il faut rester sur des règles « principielles » plutôt que de vouloir réglementer les micro-détails.

Hervé Sitruk

Ces deux textes (la DSP3 et le RSP) n'abordent pas le sujet de la souveraineté. Il y a donc un hiatus entre la réglementation et le discours politique. Aujourd'hui, on dit à la France « il y a des pays européens qui n'assurent pas leur souveraineté, vous devez donc adopter obligatoirement l'euro numérique pour que les autres puissent avancer ». On sanctionne ainsi les bons élèves qui ont investi au profit des mauvais élèves qui n'ont rien fait.

Y aura-t-il un jour un texte qui précisera ce qu'est la souveraineté européenne et ce que sont les obligations des États-membres en matière de souveraineté, de sorte que les pays qui n'ont pas de solution cherchent au moins à adopter une solution qui existe dans un autre pays européen ? Quelqu'un abordera-t-il un jour cette question ? Va-t-elle rester au niveau du politique ou va-t-elle se traduire dans les textes ?

David Sabban

Il y a plusieurs points dans ce que vous venez de dire.

Certes, le mot « souveraineté » ne figure pas dans les textes, mais quand nous négocions, côté français, dans le cadre du règlement sur le virement instantané ou du paquet DSP3-RSP, c'est quelque chose que nous avons fortement en tête. Quand on parle, par exemple, d'obligations en matière de transparence sur les paiements par carte, on voit très bien quels sont les acteurs concernés par ce type de pratique

La souveraineté des moyens de paiement est un sujet qui, il y a dix ans, n'intéressait personne. Aujourd'hui, ce sujet est abordé à bras-le-corps d'un point de vue politique, jusqu'au plus haut

niveau de l'État. C'est devenu un sujet fondamental, vu l'évolution du contexte géopolitique. Dans les textes que nous négocions, ce n'est pas parce que le terme de souveraineté n'apparaît pas qu'il ne se traduit pas par des obligations. Quand, dans les clauses de revue que j'ai mentionnées plus haut, on parle de transparence des paiements par carte ou d'inclusion des systèmes de paiement carte sur les wallets, tout cela est la traduction concrète de la notion de souveraineté. Quand on fait le virement instantané, on utilise des standards européens souverains, des infrastructures européennes, et on se désensibilise par rapport à les acteurs non-européens. C'est cela la souveraineté en actes.

La nouvelle stratégie de l'Eurosystème, qui a été présentée par Thomas Vlassopoulos lors de la Rencontre FPF du 14 avril (et que vous avez évoquée dans votre newsletter) est très intéressante sur le rôle de l'euro numérique, sur le fait de se désensibiliser d'acteurs non-européens, de privilégier des standards. Le fait que la BCE ait signé des accords pour réutiliser les standards européens, ce n'est peut-être pas très « shiny » mais c'est la souveraineté en actes.

Au-delà de la nouvelle stratégie de l'Eurosystème, que nous saluons et qui est extrêmement utile, notre souhait est que la Commission européenne actualise sa *Retail Payments Strategy* (RPS) de 2020….

Hervé Sitruk

… Absolument. En 2020, l'euro numérique n'était pas dans le paysage. C'est le paiement instantané qui était au centre de la stratégie européenne. Comment le remettre dans la photo globale ? Ce serait bien de l'expliquer. C'est d'ailleurs ce qu'a dit récemment Fernando Navarrete[2] : « il aurait fallu commencer par-là ».

David Sabban

C'est un vrai sujet que, du côté français (Bercy) nous investiguons beaucoup car nous considérons qu'il est essentiel pour les deux ou trois prochaines années.

Stéphane Mouy

J'ai une question sur le calendrier. Vous avez évoqué mi-2028 pour la mise en œuvre du futur règlement (RSP). Ce règlement prévoit des textes d'application (RTS) qui doivent être préparés

[2] Cf. interview de Fernando Navarrete le 28 avril 2026 Is Europe falling behind in global finance? - YouTube "*The ECB has come up with a strategy in payments that takes this more holistic view. I would have loved to see the process the other way round : first you have the big picture, and then you decide where to start. Here we have started with one piece, and then we realize, as Europeans that we need to do much more in other domains that are far more important*".

par l'Autorité bancaire européenne (ABE), laquelle a normalement un an pour le faire. Voyez-vous ce délai à l'intérieur de ce calendrier, ou est-ce encore plus loin ?

Hervé Sitruk

La question sous-jacente de Stéphane est « quelle sera la date d'entrée en application réelle du règlement eIDAS 2 pour les paiements ? »

David Sabban

La question du règlement eIDAS 2, du DIW, s'insère dans ce calendrier-là, mais elle est beaucoup plus avancée. Pour le paquet « paiements », nous avons les textes, mais ils ne sont pas encore entrés en application, et je n'ai pu vous donner que des dates indicatives pour leur entrée en vigueur et en application.

Sur le DIW, on a un track parallèle, mais il ne faut pas lier les deux sujets. Le RSP est assez peu disert sur ce qui a trait au DIW, parce que celui-ci répond au règlement eIDAS2. Cela suit le développement de solutions dans le cadre de ce qui est mis en place par la Commission européenne, par les différentes solutions nationales qui ont fait l'objet d'accréditations sur les différents niveaux prévus dans le texte. À Bercy, c'est la Direction générale des entreprises qui a la main sur le DIW : c'est elle qui a négocié ce texte et qui travaille avec les différents acteurs (publics et privés) qui préparent des solutions. Le RSP n'a pas vraiment d'impact sur l'utilisation du DIW.

J'en reviens à la question initiale de Stéphane Mouy sur les RTS. Nous avions eu la même question lors de transposition de la DSP2. En général, l'ABE communique un calendrier et indique quels sont les textes les plus prioritaires. Le paquet « paiements » prévoit 32 RTS (il y en avait beaucoup plus au départ mais nous avons fait un peu de « nettoyage » dans le cadre de l'agenda de simplification). Le RTS sur l'authentification forte est bien évidemment le RTS-cœur ; Il y en aura d'autres, par exemple sur l'accréditation des établissements de paiement.

Une fois les textes rendus publics, l'ABE devrait communiquer pour préparer les acteurs et leur dire « sur ce texte-là, il y aura tel calendrier de consultation ». C'est un processus classique, qu'on a vu par exemple dans le cadre du règlement MiCA : l'ABE essaie de donner de la visibilité aux acteurs sur le calendrier de préparation, de consultation et d'adoption des textes.

Marie-Agnès Nicolet

À propos des systèmes d'authentification forte, il y a des établissements qui, soit parce que ce sont de nouvelles offres, soit parce qu'ils se créent, se posent la question « Est-ce que je me mets en place un dispositif qui est celui à venir, pour éviter d'investir dans un dispositif qui est celui d'aujourd'hui ? »

David Sabban

En d'autres termes, la question est « Puis-je anticiper l'entrée en application du RSP pour la mise en place d'un dispositif d'authentification forte? ». Nous sommes encore dans le cadre de la DSP2. Il faut donc continuer à appliquer la réglementation existante. Pour le futur, les solutions d'authentification forte devront être validées par la Banque de France. En pratique, cela dépendra du calendrier de publication du RTS de l'ABE sur l'authentification forte.

Comme je l'ai indiqué plus haut, l'assouplissement prévu dans le RPS en matière d'authentification forte porte sur le facteur d'inhérence. C'est un point sur lequel, du côté du Conseil, il y a une attention forte pour éviter que cet assouplissement remette en cause la sécurité des paiements, telle qu'obtenue dans le cadre de la DSP2. Nous ne voulons pas que les nouvelles solutions d'authentification forte, qui doivent certes évoluer avec l'évolution des habitudes des consommateurs et les innovations techniques, aient pour effet de réduire le niveau de sécurité collective auquel nous avons abouti, qui est un actif très fort qu'il faut préserver car il et garant de la confiance des utilisateurs dans les moyens de paiement. Du côté de la France, en particulier du côté de la Banque de France, nous serons extrêmement vigilants là-dessus.

Pour répondre plus directement à votre question sur les investissements, cela dépendra de ce qui figurera dans les textes de l'ABE. La Banque de France participe à ces travaux, comme les autres superviseurs. Il est un peu trop tôt pour envisager ces évolutions, mais il faudra travailler en étroite coopération avec la Banque de France dans le cadre de l'OSMP et du CNMP.

Arnaud Pince

Vous avez évoqué l'open banking et FIDA. Pouvez-vous nous confirmer que le travail qui est fait dans le cadre du paquet « paiements » pour le renforcement de l'open banking, servira de socle pour FIDA (si un jour FIDA est adopté) afin d'éviter de dupliquer les dispositifs ?

David Sabban

Dans le track des négociations sur DSP3/RSP, nous avons été plus vite que sur FIDA (vous connaissez l'état des négociations sur FIDA), mais il a toujours été très clair, du côté du Conseil, que nous souhaitons la convergence.

Mais rappelons que l'open banking est gratuit, qu'il n'est pas conditionné à un accord contractuel entre ASPSP, Initiateur et Agrégateur, alors que le règlement FIDA prévoit des accords contractuels avec les schemes. On a donc une base de départ différente, et des *data holders* et *data users* beaucoup plus larges : sur l'open banking, les *data holders* sont principalement les banques ; sur l'open finance, le scope des data holders est beaucoup plus large (assureurs, CASP…).

L'idée est donc que sur le plan technique, là où la convergence peut être faite, elle doit être faite. Mais les points de départ sont tout de même différents : sur l'open finance, on est en train de créer un marché, alors que sur l'open banking, on est sur l'amélioration d'un marché existant.

Hervé Sitruk

Au niveau de l'EPC, le groupe de travail SPAA (auquel FPF participe) n'avance pas car il n'y a pas accord entre les EPAME et les banques. Comment sortir de cet imbroglio ?

David Sabban

Dans le texte initial de la Commission, il y avait une référence en matière d'accord non contractuel pour dire « si vous offrez des services premium en matière d'open banking, vous avez la possibilité de conclure des schemes ». C'était le « coup de chapeau » de la Commission au scheme SPAA. Nous étions très en soutien de ce scheme, et nous regrettons que les discussions s'enlisent.

Comme je vous l'indiquais plus haut, quand on parle de souveraineté des moyens de paiement, l'open banking ne vient pas spontanément à l'esprit. On parle de cartes ou de Wero : c'est évidemment fondamental, mais l'open banking, fait partie des instruments de paiement européens. Je regrette, par exemple, qu'il n'en soit pas fait mention explicitement dans la nouvelle stratégie des paiements de l'Eurosystème. Dans les discussions que nous pourrons avoir avec la Commission européenne sur l'actualisation de sa stratégie des paiements de détail, nous devrions essayer de relancer la dynamique autour des schemes d'open banking.

Hervé Sitruk

Il y a une question équivalente à celle des charges pour les cartes : Y a-t-il un seuil minimum ou maximum pour la facturation des services que les EPAME peuvent demander aux banques en termes d'accès aux données. Allez-vous fixer des règles ?

David Sabban

Dans ce texte-là comme dans d'autres (cf. la VoP), nous préférons privilégier la logique de scheme. Nous ne sommes pas là pour encadrer, pour prescrire des produits ou prescrire des équilibres économiques, ce n'est pas notre rôle. Donc sur les schemes, si on peut mettre un peu de pression dans le système et aider à trouver des compromis, c'est préférable.

Hervé Sitruk

Il y a des standards en matière d'API et derrière ces standards, il y a les data. Les EPAME demandent de se connecter pour accéder aux données, donc il faut qu'ils paient une prestation d'accès aux données. Mais ils disent « non, nous ne payons rien ». Il y a à la fois un

problème de standards et un problème de règles économiques. À un moment donné, il faut trancher : c'est comme un jugement de Salomon.

Emmanuelle Wisniewski

Comment avez-vous intégré l'accélération de l'IA dans votre réflexion ? Avez-vous évalué l'efficacité de votre dispositif réglementaire dans des scénarios qui peuvent arriver très rapidement ?

David Sabban

Nous évoluons effectivement dans un environnement technologiquement très dynamique, avec une accélération très forte du cycle d'innovation en matière de paiements, notamment les problématiques d'IA qui, lorsque le texte a commencé à être négocié en 2023, n'étaient pas encore identifiées comme importantes.

Notre logique en matière de textes financiers est toujours de rester à un niveau « principiel ». Un des pièges dans lesquels les régulateurs essaient de pas tomber est de chercher à avoir un texte qui s'adapte constamment à l'innovation technologique. Si cela avait été le cas, le paquet « paiements » n'aurait jamais été adopté.

Je vais reprendre l'exemple évoqué plus haut de la lutte contre la fraude. Quand on parle de *transaction monitoring mechanisms*, on sait que ces mécanismes reposent et sont nourris par de l'intelligence artificielle, dans les logiciels, dans les dispositifs internes aux banques et aux PSP. La façon dont les textes sont pensés et négociés ne consiste pas à dire « l'IA doit faire ceci ou cela », mai à dire « ces mécanismes doivent permettre de… ».

Autre point qu'il faut avoir en tête : nous avons notre texte sectoriel « paiements », mais l'IA Act a une portée très large qui s'applique au secteur financier et aux secteurs non financiers, L'idée est, ici aussi, d'aboutir à des règles « principielles » qui ne soient pas trop prescriptives et trop détaillées.

Mais bien évidemment, les problématiques de fraude renforcées par l'IA seront placées très haut dans l'agenda de la plateforme européenne de lutte contre la fraude. On apprend en marchant ; les textes doivent aussi être éprouvés, et ils ne sont pas là pour l'éternité une fois qu'on les a adoptés. Il y aura un RSP2, il y aura une DSP4.

Hervé Sitruk

La Commission a engagé la révision de l'IA Act. Par ailleurs, le marché avance, beaucoup plus vite qu'on ne le pense (Google et Mastercard soutiennent l'application de Fido dans le monde de l'agentique), et nous sommes encore en train de nous poser la question… .

David Sabban

Quand on a fait l'authentification forte, on a fixé des grandes règles (connaissance, inhérence, possession). Plus ces règles restent « principielles », plus elles seront en capacité de s'adapter aux évolutions de l'environnement technologique. C'est un point important.

Hervé Sitruk

Merci à nouveau, David.

****