Compte rendu officieux NdS (Projet, V1)

Marie-Agnès Nicolet

Le rapport annuel de contrôle interne (RACI) comporte cette année une annexe dans laquelle les prestataires de services de paiement doivent indiquer comment ils se conforment aux recommandations de l'Observatoire de la sécurité des moyens de paiement (OSMP).

1. **Contexte : Le Rapport Annuel du Contrôle Interne**

- **L'annexe au Rapport annuel de contrôle interne (RACI) relative à la sécurité des moyens de paiement scripturaux et de l'accès aux comptes, transmise chaque année par les PSP avant le 30 avril, a évolué en 2026 au titre de l'exercice 2025.**
- **Ces nouvelles exigences intègrent particulièrement les recommandations de l'Observatoire de la sécurité des moyens de paiement (OSMP), qui constituent le référentiel de place en la matière.**
- **Les évolutions introduites par le nouveau canevas du RACI de l'ACPR impliquent ainsi une analyse structurée de l'alignement des dispositifs de l'établissement avec les recommandations de l'OSMP applicables.**

Nous sommes heureux d'accueillir ce matin Pierre Bienvenu, chef du service des moyens de paiement scripturaux (SPMS) à la Banque de France et sa collègue Marine Soubielle, qui vont nous éclairer sur les attentes de l'OSMP et de la Banque de France en la matière.

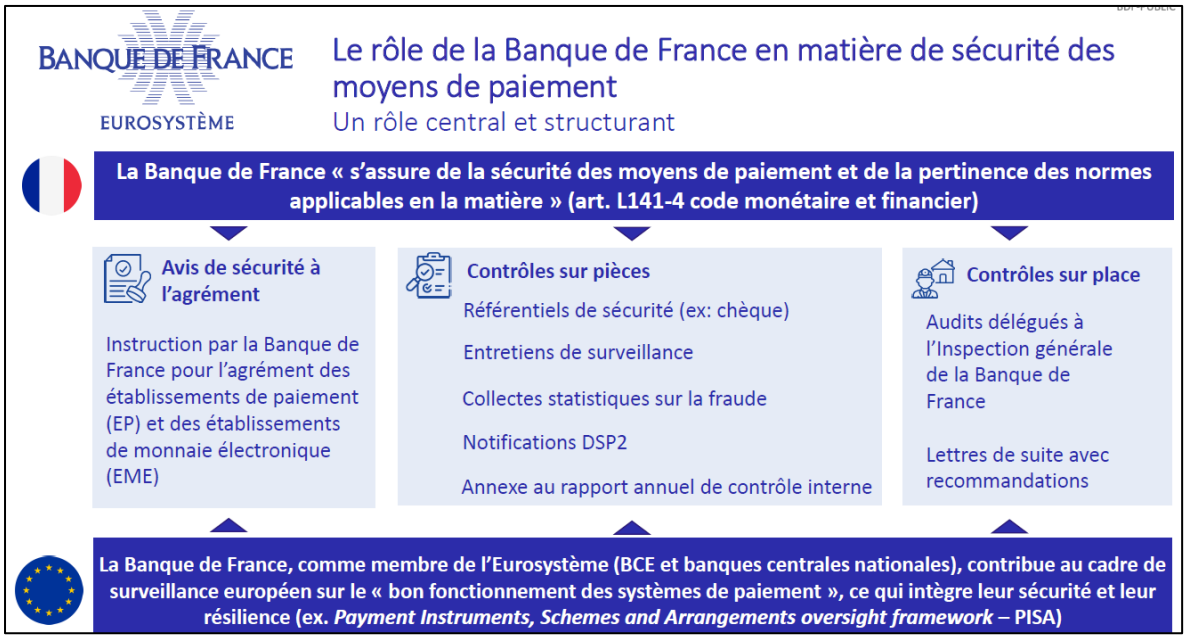
Pierre Bienvenu

Merci à France Payment Forum d'organiser cet échange : il est très important pour nous d'être en lien avec les acteurs de marché, non seulement les grands établissements bancaires mais aussi les autres prestataires de services de paiement.

Depuis 2001, la Banque de France s'est vu confier par le législateur la mission de s'assurer de la sécurité des moyens de paiement et de la pertinence des normes applicables en la matière. Cette mission a naturellement un lien avec la confiance dans la monnaie. Pour avoir confiance dans la monnaie, il faut bien sûr une inflation aussi maîtrisée que possible, mais il faut aussi avoir confiance dans les moyens d'utiliser cette monnaie au quotidien, c'est-à-dire les moyens de paiement.

Comment cette mission s'organise-t-elle ?

- **Via des avis de sécurité à l'agrément**. Au moment de l'agrément par l'ACPR des établissements de paiement et des établissements de monnaie électronique, la Banque de France rend un avis sur la sécurité de l'établissement candidat à l'agrément ou candidat à l'extension de l'agrément.



- **Via des contrôles sur pièces** qui s'articulent autour de nos référentiels de sécurité, l'essentiel de référentiels étant maintenant européens (le seul référentiel national étant le référentiel de sécurité sur le chèque). Nous organisons aussi des entretiens de surveillance, et nous collectons des statistiques sur l'usage des moyens de paiement et sur la fraude. Et il y a notamment cette annexe au rapport annuel de contrôle interne (RACI), qui est adressée à l'ACPR.
- **Et via des contrôles sur place.** Ces contrôles sont délégués à l'Inspection générale de la Banque de France. À la suite de ces contrôles sur place, des lettres de suite sont émises, avec des recommandations.

Tout cela s'effectue en interaction permanente avec le cadre européen. Au titre des Traités européens, les banques centrales de l'Eurosystème sont en effet en charge du bon fonctionnement des systèmes de paiement, et cette mission se décline aussi par un cadre de surveillance sur la sécurité et la résilience des « *schemes and arrangements* », c'est-à-dire Visa, Mastercard, Carte Bancaire, Apple Pay… tous ces systèmes qui sont utilisés au quotidien par les citoyens européens pour leurs paiements.

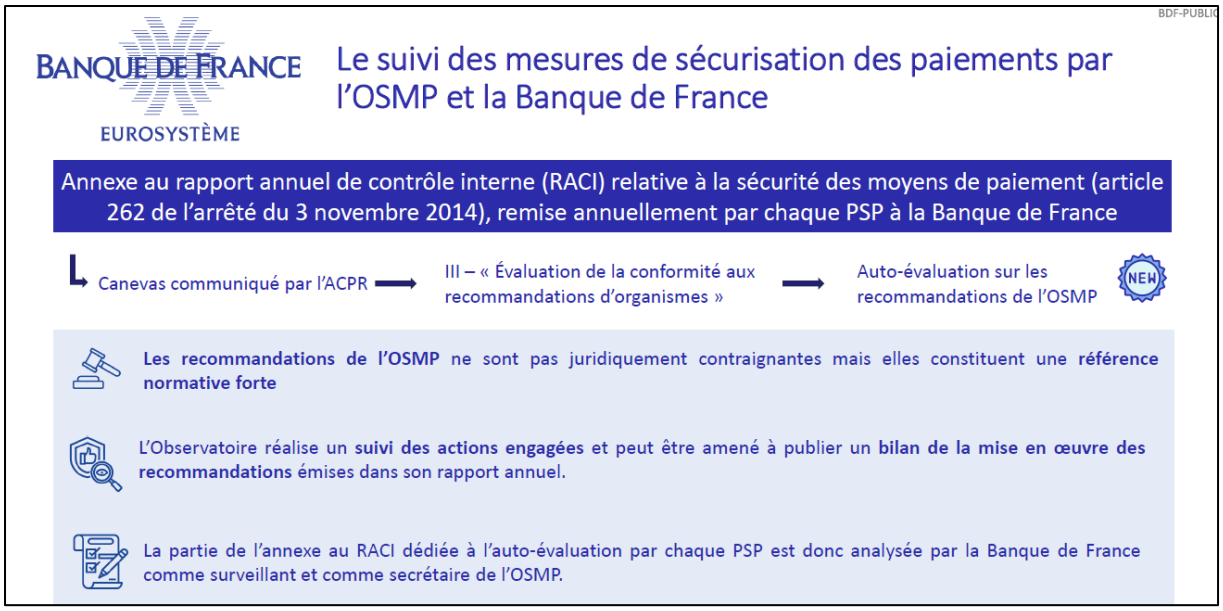
À la différence de l'ACPR, cette mission de surveillance n'est pas associée à un pouvoir de sanction. On parle classiquement de « persuasion morale », notre objectif étant, en lien avec les acteurs de marché, de les convaincre de la pertinence de nos recommandations.

Marine Soubielle

Présidé par le premier sous-gouverneur de la Banque de France, l'OSMP est un forum chargé de promouvoir le dialogue et les échanges d'informations entre les différents acteurs qui sont à la fois concernés par la sécurité et le bon fonctionnement des moyens de paiement, mais aussi par la lutte contre la fraude. Il rassemble les différents représentants de l'écosystème des paiements.

Les trois missions confiées à l'OSMP par la loi (cf. article L141-4 du Code monétaire et financier) sont :

- Le suivi des mesures de sécurisation des paiements mises en œuvre par les émetteurs, les commerçants et les entreprises,
- L'établissement des statistiques de fraude,
- La veille technologique, pour proposer des moyens de lutter contre les atteintes à la sécurité des moyens de paiement.



Le suivi des mesures de sécurisation des paiements prend souvent la forme de recommandations ou de plans d'action. Ces recommandations n'ont pas de valeur contraignante (au sens juridique), mais les banques et les PSP sont fortement incités à s'y conformer et lors de ses contrôles, l'ACPR peut se reposer sur ces recommandations. Celles-ci ont donc une portée « quasi réglementaire ». Le suivi des mesures de sécurisation fait l'objet d'un bilan qui est présenté dans les rapports annuels de l'OSMP.

La Banque de France a décidé d'intégrer une grille d'auto-évaluation de chacun des PSP dans l'annexe au rapport annuel de contrôle interne (RACI) relative à la sécurité des moyens de paiement, afin que ces PSP puissent faire un état des lieux de leurs avancées sur ces recommandations et que la Banque de France puisse faire un suivi rapproché de chacun de ces PSP.

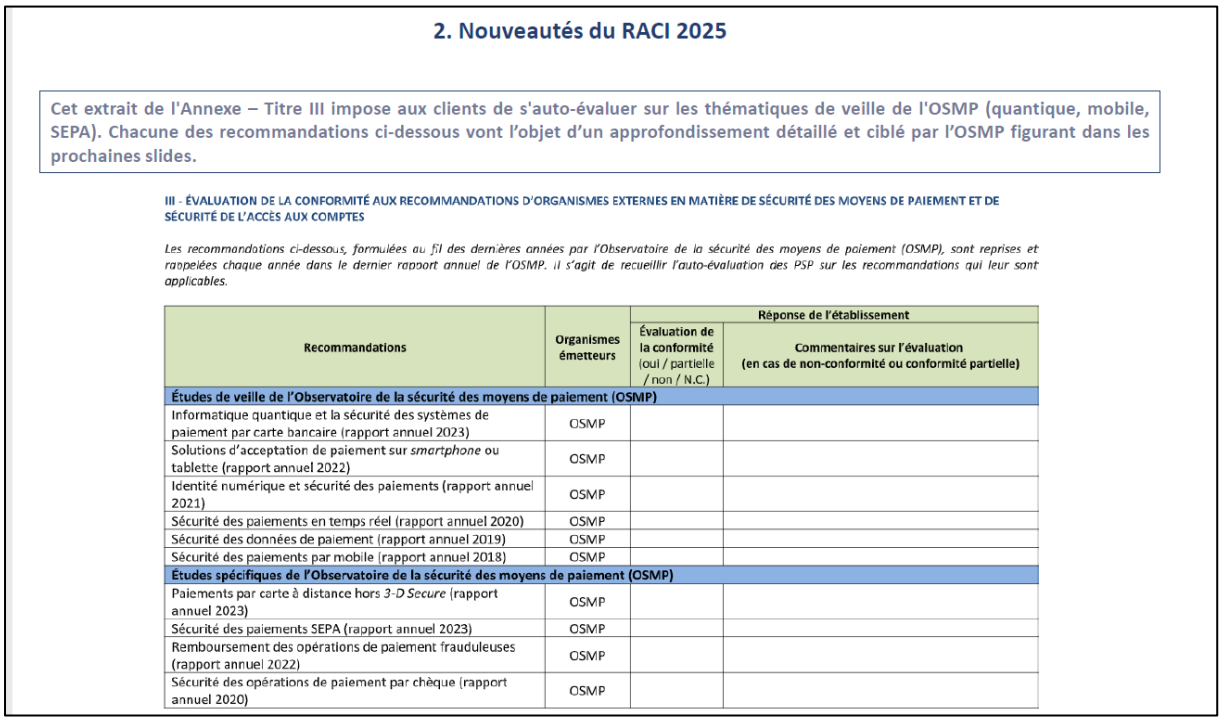
Pierre Bienvenu

La Banque de France et l'Observatoire, même s'il s'agit de deux personnalités juridiques distinctes, se complètent mutuellement : il y a nécessairement une cohérence entre la surveillance exercée par la Banque de France et les objectifs poursuivis par l'Observatoire, puisque la Banque de France préside l'Observatoire et en assure le secrétariat.

Mais l'Observatoire a une dimension collégiale : les PSP y sont représentés, de même que les commerçants, les utilisateurs, les administrations, la CNIL, l'ANSSI… Dès lors que les recommandations de l'Observatoire ont été validées par l'ensemble de l'écosystème, la Banque de France les intègre dans son programme de surveillance. Et pour bien diffuser ces recommandations, il nous a paru important de réintégrer cette auto-évaluation dans l'annexe du RACI.

Marie-Agnès Nicolet

Dans l'annexe du RACI 2025, le PSP doit indiquer s'il est conforme ou non, ou partiellement conforme, mais je comprends que certains sujets issus de rapports un peu anciens sont parfois arrivés dans la réglementation et que sur certains sujets nouveaux, on est plutôt parfois avec l'idée d'un plan d'action à mettre en place.



2. Nouveautés du RACI 2025

Cet extrait de l'Annexe – Titre III impose aux clients de s'auto-évaluer sur les thématiques de veille de l'OSMP (quantique, mobile, SEPA). Chacune des recommandations ci-dessous vont l'objet d'un approfondissement détaillé et ciblé par l'OSMP figurant dans les prochaines slides.

III - ÉVALUATION DE LA CONFORMITÉ AUX RECOMMANDATIONS D'ORGANISMES EXTERNES EN MATIÈRE DE SÉCURITÉ DES MOYENS DE PAIEMENT ET DE SÉCURITÉ DE L'ACCÈS AUX COMPTES

Les recommandations ci-dessous, formulées au fil des dernières années par l'Observatoire de la sécurité des moyens de paiement (OSMP), sont reprises et rappelées chaque année dans le dernier rapport annuel de l'OSMP. Il s'agit de recueillir l'auto-évaluation des PSP sur les recommandations qui leur sont applicables.

Recommandations	Organismes émetteurs	Réponse de l'établissement	
		Évaluation de la conformité (oui / partielle / non / N.C.)	Commentaires sur l'évaluation (en cas de non-conformité ou conformité partielle)
Études de veille de l'Observatoire de la sécurité des moyens de paiement (OSMP)			
Informatique quantique et la sécurité des systèmes de paiement par carte bancaire (rapport annuel 2023)	OSMP		
Solutions d'acceptation de paiement sur *smartphone* ou tablette (rapport annuel 2022)	OSMP		
Identité numérique et sécurité des paiements (rapport annuel 2021)	OSMP		
Sécurité des paiements en temps réel (rapport annuel 2020)	OSMP		
Sécurité des données de paiement (rapport annuel 2019)	OSMP		
Sécurité des paiements par mobile (rapport annuel 2018)	OSMP		
Études spécifiques de l'Observatoire de la sécurité des moyens de paiement (OSMP)			
Paiements par carte à distance hors *3-D Secure* (rapport annuel 2023)	OSMP		
Sécurité des paiements SEPA (rapport annuel 2023)	OSMP		
Remboursement des opérations de paiement frauduleuses (rapport annuel 2022)	OSMP		
Sécurité des opérations de paiement par chèque (rapport annuel 2020)	OSMP		

Ainsi par exemple, dans le rapport annuel 2023 de l'OSMP, il y a des sujets sur l'informatique quantique et la sécurité des systèmes de paiement par carte.

On sait que les ordinateurs quantiques vont bouleverser la donne et permettre de « craquer » des clés cryptographiques. Dans les recommandations de l'OSMP, il est question d'anticiper ce risque quantique en cartographiant les vulnérabilités, en hiérarchisant les données sensibles, en expérimentant de nouveaux algorithmes asymétriques, en élaborant une feuille de route.

On voit que là-dessus, les PSP ne sont pas encore complètement dans le sujet, qui est très nouveau. La Place commence à se mobiliser en se disant que c'est maintenant (et pas dans 5 ans) qu'il faut commencer à traiter le sujet, mais peu d'entre eux ont des plans d'action. Qu'attendez-vous sur ce sujet ?

Pierre Bienvenu

La mission de l'Observatoire est d'être en anticipation des risques futurs. Quand l'OSMP a décidé, en 2023, de parler du quantique, il a mis en place un groupe de travail avec différents acteurs de l'écosystème, des spécialistes de la cryptographie…Quand nous émettons des recommandations là-dessus, nous ne nous attendons pas nécessairement à ce que tous les établissements soient en conformité stricte par rapport à ces recommandations. Mais c'est en anticipation de ces risques futurs et face à l'incertitude que l'Observatoire dit que l'écosystème doit se mobiliser dès maintenant.

Une recommandation « basique » est donc de lire l'étude qui figure dans le rapport annuel 2023 de l'OSMP car au-delà de remplir l'annexe au RACI, cette étude est, à notre sens, une porte d'entrée pour tous les PSP sur ces nouveaux sujets complexes.

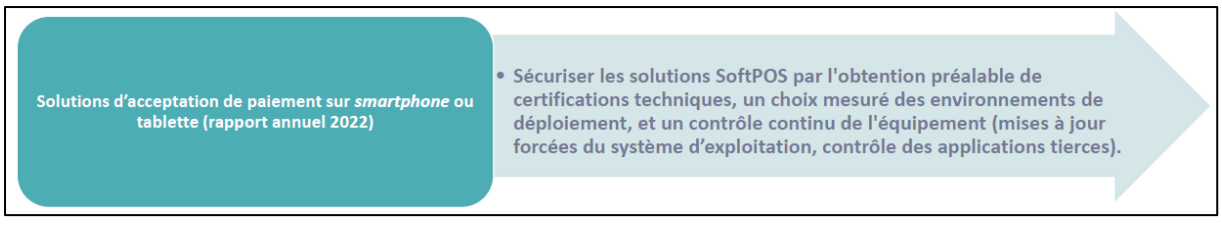
Ensuite, les recommandations sont destinées à l'écosystème des paiements : les PSP bien sûr, mais aussi les systèmes de paiement par carte. On sait que Carte bancaire est en train d'élaborer une feuille de route pour se préparer à l'informatique quantique.

Donc pour ces recommandations-là, nous ne nous attendons pas forcément à une conformité stricte : il peut y avoir une conformité partielle, mais ce que nous souhaitons, c'est que les PSP se saisissent de ce sujet et fassent autant que possible ces cartographies des vulnérabilités. Cela prendra du temps, mais il faut être prêt quand l'informatique quantique sera mature et pourra casser les clés cryptographiques actuelles.

Bien sûr, cela dépend de chaque établissement, de son modèle d'activité, du recours ou non à des prestataires… Mais le fait de se poser la question est déjà une première étape.

Cathie-Rosalie Joly

La deuxième thématique concerne l'acceptation des paiements sur les smartphones ou les tablettes (solutions dites « SoftPOS »), c'est-à-dire des logiciels de télépaiement installés sur un matériel qui n'a pas été conçu à l'origine pour l'acceptation des paiements. Ces travaux ont été engagés par l'OSMP dès 2016 et ont abouti aux recommandations qui ont été publiées dans le rapport 2022, où il est fait référence à l'obtention d'une certification technique avant d'expérimenter le SoftPOS, à des choix sur les environnements de déploiement pour le SoftPOS, à des recommandations sur la mise en place de programmes d'action et de contrôle pour s'assurer de la sécurité de la mise en place des SoftPOS, avec aussi des préconisations sur la formation des commerçants et sur les obligations de veille.



Vous indiquiez que certaines recommandations de l'OSMP sont plutôt des préconisations ou incitations alors que d'autres sont quasi-impératives. Dès lors, sur cette question des SoftPOS, qu'attendez-vous des PSP ? Quelles certifications sont-elles absolument indispensables (PCI, EMV…) ? Par quelle autorité certificatrice (ANSSI ou autre) ? A-t-on des informations sur les contextes de déploiement que vous estimez compatibles pour la mise en place de SoftPOS, en termes montant ou de types de commerces ?

Pierre Bienvenu

L'étude de 2016 à laquelle vous faisiez allusion portait sur les nouveaux types de boîtiers qui permettaient l'acceptation des paiements par carte. Mais dans l'étude publiée dans le rapport 2022, on était vraiment sur le smartphone en tant que tel, donc les solutions dites SoftPOS. Quand nous avons fait cette étude en 2022, ces solutions étaient encore extrêmement marginales. Mais pour les PSP qui déploient ce type de solution en tant que PSP acquéreurs, les recommandations de l'OSMP ont un pouvoir normatif fort : notre attente est que les PSP qui déploient ce type de solution s'y conforment.

La principale recommandation était d'être sélectif dans le déploiement de ces solutions : là où on a une expérience éprouvée avec les terminaux classiques (qui eux-mêmes se modernisent de plus en plus), notre point de vue est qu'il ne faut pas les abandonner du jour au lendemain pour basculer tout son parc de terminaux sur du smartphone. Mais dès lors qu'un PSP acquéreur déploie ce type de solution, oui, les recommandations sont à suivre.

J'en profite pour rappeler que les recommandations de l'Observatoire s'adressent aux PSP, mais pas seulement : il y a aussi des recommandations qui s'adressent aux utilisateurs ou aux commerçants. Une partie de la sécurité de ces solutions SoftPOS repose aussi sur les commerçants et consiste par exemple à leur dire : « évitez de mélanger usage professionnel et usage personnel, faites en sorte que le smartphone utilisé comme SoftPOS puisse être distingué des autres, qu'il soit mis en lieu sûr le soir après la fermeture du magasin… ».

Cathie-Rosalie Joly

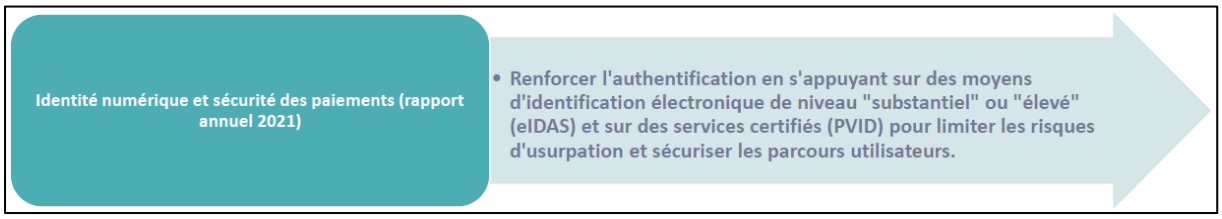
Cela veut-il dire que dans leurs réponses au RACI, les PSP doivent expliquer leur approche par les risques en matière d'acceptation des SoftPOS, les contrôles et les échanges ou formations mis en place avec les commerçants ?

Pierre Bienvenu

Dans chaque rapport annuel, nous essayons de reprendre *in extenso* toutes les recommandations dans un chapitre dédié, et on voit bien celles qui sont destinées aux PSP, celles qui sont destinées aux commerçants et celles qui sont destinées aux utilisateurs. La diffusion des recommandations repose aussi sur les actions de sensibilisation des PSP auprès de leurs propres clients.

Arnaud Pince

La troisième recommandation mentionnée dans l'annexe du RACI est relative à l'identité numérique et à la sécurité des paiements. L'Observatoire soulignait dans son rapport 2021 le rôle croissant des mécanismes d'identification électronique dans les parcours de paiement, notamment lors de l'entrée en relation et de l'identification à distance.



L'une des recommandations aux PSP était de renforcer les mécanismes d'authentification lors de l'entrée en relation en s'appuyant davantage sur des moyens d'identification électronique de niveau substantiel ou élevé, au sens du règlement eIDAS, ou de recourir à des services certifiés d'entrée en relation à distance proposés par les prestataires de vérification d'identité à distance, les PVID. Or, depuis ce rapport 2021, le cadre réglementaire a évolué avec le déploiement progressif de eIDAS2 et du futur portefeuille européen d'identité électronique. Dans ce contexte, quelles sont les recommandations de l'Observatoire qui demeurent valables, comment vont-elles évoluer au regard de la réglementation eIDAS2 notamment ?

Pierre Bienvenu

La réglementation prime. Le message de l'Observatoire est que parmi les différentes solutions d'enrôlement d'un client, il peut y avoir deux solutions conformes d'un point de vue de la réglementation mais dont une est potentiellement plus sûre que l'autre contre la fraude. Les PSP sont invités à aller vers les solutions les plus sûres, dès lors qu'elles sont conformes à la réglementation.

Au-delà de cette question de l'enrôlement de nouveaux clients, cette étude portait aussi sur les services de signature électronique, de cachet électronique, qui peuvent aussi sécuriser les échanges dans d'autres usages tels que les échanges entre les PSP et les commerçants, entre les PSP et les entreprises, ou entre les entreprises et les consommateurs.

Et bien sûr, il y a cette actualité avec eIDAS 2, que nous traiterons ultérieurement, mais je pense que même s'il y a eu des évolutions depuis, l'essentiel des recommandations est encore largement valable.

Hervé Sitruk

C'est un sujet qui a fait l'objet d'une réunion entre France Payment Forum et la Banque de France (Julien Lasalle et Pierre Bienvenu), avec également des représentants d'EPI et de b.connect. Le Règlement eIDAS2 impose pour fin 2027 que si un utilisateur veut utiliser l'identité numérique pour l'authentification, il puisse le faire. Ce n'est donc pas une

généralisation pour l'authentification, mais une possibilité offerte aux utilisateurs, ce qui implique que tous les PSP puissent offrir le service à ceux qui disposent de cette identité numérique.

La France est très en retard sur d'autres pays européens en ce domaine. FRANCE PAYMENTS FORUM va organiser en avril une rencontre digitale sur l'identité numérique, avec des représentants de France Identité, mais aussi des solutions belge et allemande pour montrer que dans d'autres pays ce sujet avance vite. Nous souhaitons que l'OSMP prenne en charge ce sujet parce que la France est véritablement en retard dans ce domaine.

Nous avions beaucoup apprécié cette étude de l'OSMP, mais depuis lors le contexte a fondamentalement changé. Il y a une obligation pour fin 2027 (même si c'est décalé du fait du retard de beaucoup de pays, dont la France), et nous souhaitons que l'OSMP reprenne pied sur ce sujet.

Pierre Bienvenu

C'est bien prévu. Dans le rapport annuel 2024, l'étude de veille portait sur l'intelligence artificielle dans le scoring de fraude. L'étude de veille que nous avons lancée en janvier porte sur les nouvelles solutions d'authentification et dans ces nouvelles solutions, nous couvrirons à la fois les solutions du type Click-to-Pay mais aussi l'interaction entre l'authentification forte au sens de la DSP2 et les portefeuilles d'identité électronique au sens d'eIDAS. Nous allons donc essayer de vulgariser tout cela dans la prochaine étude de veille de l'Observatoire, qui a été lancée en janvier 2026.

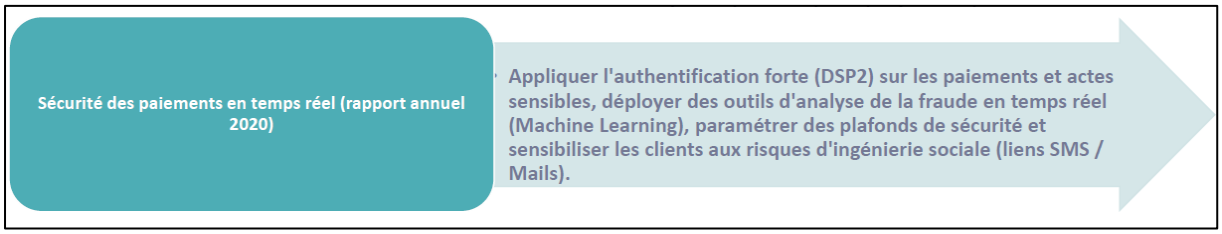
Sur l'identité numérique, effectivement, il y a ce qui est qualifié au sens d'eIDAS (ce qui peut être bien dans certains usages et renforcer la sécurité), mais il y a d'autres choses qui ne seront pas qualifiées au sens d'eIDAS, comme par exemple b.connect, qui sont aussi très bien pour renforcer la sécurité de certains parcours du point de vue des commerçants. Les recommandations de l'OSMP portaient aussi sur les opérateurs de téléphonie mobile afin qu'ils renforcent leur parcours client quand ils délivrent de nouvelles cartes SIM ou quand ils ouvrent de nouvelles lignes mobiles.

Les recommandations ne sont donc pas seulement à l'intention des PSP, mais le message principal vis-à-vis des PSP est que l'enrôlement et l'ouverture de compte sont des processus critiques, non seulement d'un point de vue conformité, mais aussi d'un point de vue de sécurité générale de l'écosystème pour lutter contre la fraude, sachant qu'une bonne partie de la fraude aux virements repose aujourd'hui sur l'ouverture de compte frauduleux.

Marie-Agnès Nicolet

Cela nous fait une bonne transition avec les recommandations du rapport de 2020 sur la sécurité des paiement en temps réel. Il était recommandé d'appliquer l'authentification forte. Aujourd'hui, c'est dans les textes, mais comme cela va changer, en termes de critères, avec la

DSP3, les établissements qui travaillent aujourd'hui sur la mise en place de certains systèmes peuvent-ils être sur les nouveaux critères ?



Concernant la recommandation de déployer des outils d'analyse de la fraude en temps réel en utilisant du *machine learning*, donc de l'IA, jusqu'où pensez-vous que les établissements doivent aller en la matière ?

Ensuite, il y a dans cette recommandation des éléments plus faciles à mettre en œuvre, comme le paramétrage des plafonds de sécurité et la sensibilisation des clients aux risques d'ingénierie sociale, puisqu'on voit parfois des établissements mis en cause par des clients qui ont été victimes d'une fraude au président ou au faux conseiller.

Pierre Bienvenu

Quand nous avons émis cette recommandation en 2020, nous étions dans l'anticipation des risques car à l'époque le virement instantané n'était pas aussi déployé qu'il l'est aujourd'hui.

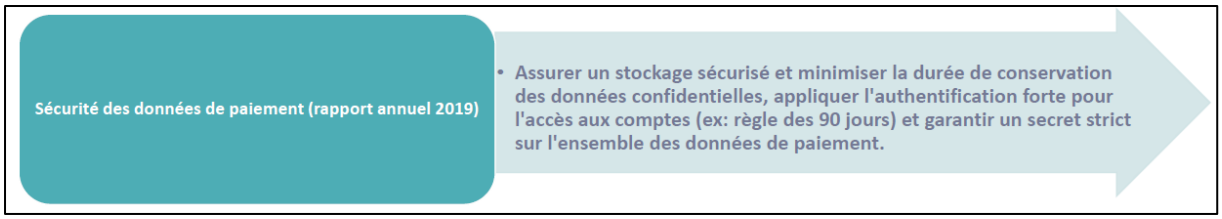
Les outils d'analyse de la fraude en temps réel sont quasiment une obligation. Ils le seront encore plus fortement avec la DSP3 et le RSP quand ils seront entrés en application. Tout le monde est conscient qu'il faut utiliser des outils d'IA pour mieux détecter les risques de fraude.

Sur les plafonds de sécurité, la recommandation de l'Observatoire va un peu plus loin que la réglementation puisqu'elle dit qu'il faut ajuster les plafonds sur le virement instantané en fonction des besoins du client. Les plafonds sur le virement instantané sont encore trop souvent quasiment uniformes, quel que soit le client. Ils ne sont pas du tout aussi adaptés que peuvent l'être les plafonds de paiement par carte. Or cette personnalisation des plafonds nous paraît essentielle pour limiter les préjudices et renforcer la sécurité du virement instantané.

Donc cette recommandation du rapport 2020 reste largement valable : même si le taux de fraude du virement instantané est sous contrôle, il faut s'inscrire dans un dispositif d'amélioration continue.

Marie-Agnès Nicolet

J'en viens à la recommandation issue du rapport 2019 sur la sécurité des données de paiement. Comme vous l'avez rappelé, pour les dossiers d'agrément, par exemple, d'établissement de paiement et de monnaie électronique la Banque de France examine leurs dispositifs de sécurité. Quelle est l'articulation avec la politique de sécurité des données de paiement, dans un contexte où DORA introduit également des exigences de sécurité.



Cathie-Rosalie Joly

Il y a effectivement une juxtaposition d'exigences réglementaires. Faut-il multiplier les politiques de sécurité avec des objectifs différents ? La bonne pratique n'est-elle pas plutôt de centraliser, avec un cœur d'exigences de sécurisation commun à l'ensemble de ces textes, et de traiter par exception les points de différenciation ?

Pierre Bienvenu

C'est plutôt la deuxième solution. Depuis l'époque où nous avons fait cette étude en 2019, il y a eu DORA et aussi le RGPD. Pour l'Observatoire, l'essentiel est la sécurité des données de paiement : les données de cartes, mais aussi les IBAN. La sécurité des IBAN est un point sur lequel nous sommes très attentifs lorsque nous examinons les dossiers d'agrément des PSP. Et l'actualité toute récente montre que la sécurité des IBAN ce n'est pas seulement chez les PSP, mais aussi chez les administrations (ainsi que chez les entreprises et chez les commerçants).

Pour répondre plus directement à votre question : nous ne sommes pas pour la sédimentation et la complexité réglementaire ; nous souhaitons que les recommandations de l'Observatoire s'intègrent autant que possible dans les dispositifs existants, les enrichissent.

Cathie-Rosalie Joly

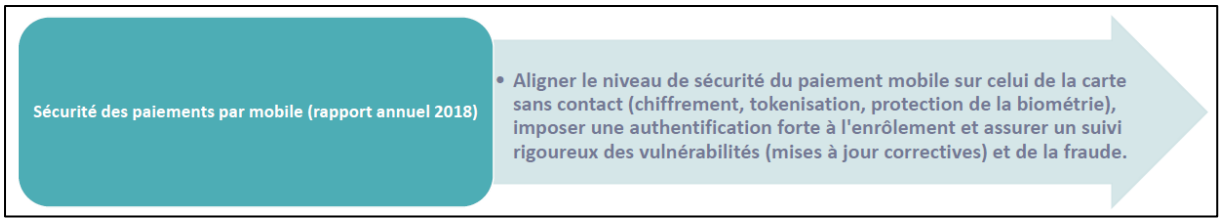
La Banque de France et l'OSMP arriveront-ils à pousser la mise en place d'un équivalent européen de l'OSMP?

Pierre Bienvenu

Le projet de règlement sur les services de paiement (RSP) prévoit un OSMP européen, qui s'appellerai « *Platform on Combating Fraud* » dont la présidence et le secrétariat seront assurés par la Commission européenne.

Cathie-Rosalie Joly

Venons-en à la recommandation de l'OSMP concernant la sécurité des paiements mobiles. Vous évoquiez précédemment la question de l'entrée en relation et de l'enrôlement. Nous pourrions peut-être faire un focus sur l'enrôlement de la carte dans les wallets. Il y a une recommandation impérative sur l'authentification forte lors de l'enrôlement, mais aussi d'autres recommandations plus anciennes, puisqu'elles remontent au rapport 2018.



Pierre Bienvenu

Il pourrait certes y avoir des ajustements dans la future réglementation, mais ces recommandations restent largement valables. Par exemple, dans le rapport 2018, nous rappelions la nécessité d'une authentification forte à l'enrôlement. Cette recommandation s'appuyait à l'époque sur le cadre de la DSP2, mais jusqu'en 2023-2024, certains fournisseurs de solutions de paiement mobile ne permettaient pas cette authentification forte à l'enrôlement, de sorte que pendant quelques années la fraude sur le paiement mobile a été bien supérieure à ce qu'elle aurait dû être.

Ceci montre qu'il faut parfois un peu insister et dans ce cas précis il a même fallu que l'Autorité bancaire européenne « mette les points sur les i » pour rappeler cette obligation d'authentification forte à l'enrôlement.

Cathie-Rosalie Joly

Avez-vous des attentes spécifiques sur ce sujet à l'égard des fabricants de smartphones, des éditeurs d'OS ?

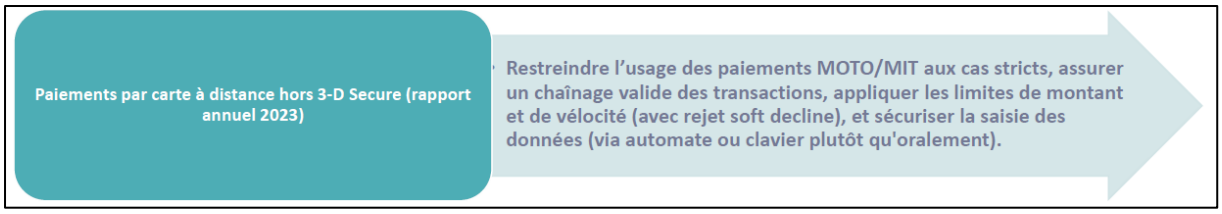
Pierre Bienvenu

Non : nous avons d'autres sujets à traiter avec les fabricants de smartphone, mais nous n'avons pas de suivi spécifique sur ce sujet-là.

Ici, nous parlons des recommandations destinées aux PSP et sur lesquelles nous attendons leur retour, notamment dans les contrats qu'ils peuvent avoir avec ces fournisseurs de solutions de paiement mobile. Les PSP restent responsables et nous leur rappelons la réglementation applicable en la matière.

Cathie-Rosalie Joly

Le point suivant concerne les paiements à distance hors 3D Secure. Vous rappelez l'obligation de mettre en place de l'authentification sur les paiements à distance, avec des cas très restreints d'exemption prévus par les RTS. Dans le rapport, vous avez constaté des taux de fraude plus élevés pour les paiements à distance hors 3DS, et particulièrement les paiements initiés par le commerçant (paiements MIT) et les paiements par courrier ou téléphone (paiements MOTO) pour lesquels il n'y a pas d'authentification du porteur lors des transactions.



Beaucoup de recommandations ont été formulées sur ce point, notamment pour limiter les cas d'usage de paiements MIT et MOTO, pour prévoir une référence complète de chaînage des transactions MIT, des recommandations sur des limites de vélocité, sur la mise en œuvre du *soft decline*, une extension potentielle aux transactions « *one-leg* ». Il y a donc de nombreuses recommandations sur ce thème : ont-elles toutes le même niveau impératif ?

Pierre Bienvenu

Ici, nous allons plus loin que la réglementation, car il y a clairement des points de vulnérabilité sur les paiements par carte hors 3DS. Nous recommandons donc la quasi-généralisation de l'usage 3DS pour les paiements sur Internet. Et il faut que toute la chaîne (l'acquéreur, l'émetteur, le commerçant…) s'inscrive dans cette dynamique. Celle-ci est pour l'essentiel impulsée par les grands groupes bancaires français, mais notre attente est que les PSP autres que ces grands groupes s'inscrivent également dans cette même dynamique.

Concrètement, notre attente est que pour les paiements sur Internet, l'usage de 3DS soit systématique, du moins pour les paiements européens. Pour les paiements internationaux, il y a quelque chose de plus progressif, parce que quand on fait un paiement vis-à-vis des États-Unis, l'usage du 3DS est plus incertain, mais nous avons une feuille de route qui dit que d'ici fin 2026, un paiement vers les États-Unis sera refusé si le montant est supérieur à 500 euros.

Pour les paiements MOTO, nous soutenons l'écosystème pour qu'il mette en place une solution d'authentification des paiements TO (*telephone order*). Notre attente est que les paiements MOTO soient aussi restreints que possible, et que d'autres canaux de plus sûrs, tels que les paiements par lien ou par virement, soient privilégiés.

Cathie-Rosalie Joly

Sur ces questions, comme vous l'avez souligné, vous allez plus loin que la réglementation. Cela a pour incidence que les PSP français sont invités à les respecter, ce qui implique pour eux un coût en termes de procédures, de développements techniques et de gestion opérationnelle. Comment prenez-vous en compte le caractère obligatoire de ces dispositions selon qu'il s'agit d'un établissement français ou d'un établissement d'un autre pays européen ?

Pierre Bienvenu

Ici, nous sommes dans le registre de la persuasion morale. Cela induit certes des coûts, mais il y a aussi les bénéfices, que nous mesurons d'ores et déjà : le taux de fraude sur les paiements

par carte s'améliore significativement et une grande partie de cette baisse du taux de fraude est liée à ce plan d'action de l'Observatoire.

Nous continuerons aussi sur la partie MOTO. Celle-ci n'étant pas traitée dans le RSP, nous ne sommes pas intransigeants sur la date de mise en conformité, mais volontaristes quant à la dynamique dans laquelle il faut s'inscrire.

Cathie-Rosalie Joly

Sur ces sujets non traités dans le RSP, pour parvenir à une harmonisation et un renforcement de la sécurisation, la bonne instance ne serait-elle pas l'OSMP européen ?

Pierre Bienvenu

Peut-être. La logique de l'Observatoire est d'agir de façon aussi agile que possible avec l'ensemble de l'écosystème. Sur ce sujet, nous avons vu qu'il y avait un point à traiter et une volonté autour de la table de le traiter. Donc nous le traitons sans attendre les évolutions réglementaires au niveau européen.

Pour moi, c'est une illustration parfaite de la force de l'Observatoire : nous traitons les choses au niveau français et peut-être cela inspirera-t-il demain des dispositifs européens. Au niveau français, la dynamique est très positive, et Visa et Mastercard commencent à se dire « on a déployé cela en France, cela marche, et d'autres régulateurs européens devraient peut-être s'en inspirer ». Dans le même ordre d'idées, la loi Labaronne contre la fraude bancaire est une initiative française qui anticipe ce qui sera demain dans le RSP.

Cathie-Rosalie Joly

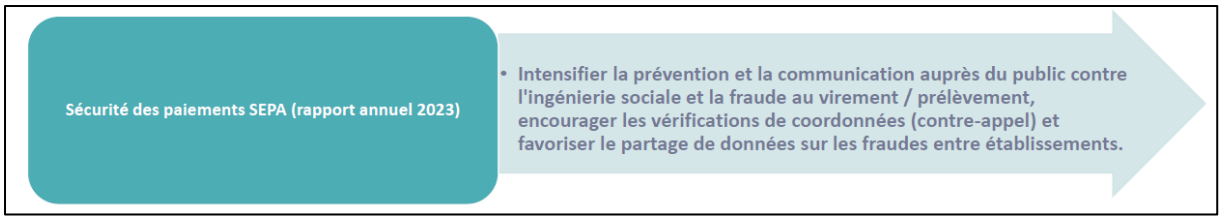
Je retiens que vous n'attendez pas forcément des PSP une conformité complète à l'ensemble des recommandations de l'OSMP, mais qu'ils se soient inscrits dans la démarche et aient commencé à mettre en place des briques de sécurisation.

Pierre Bienvenu

Exactement. Ce plan d'action ayant désormais près de deux ans d'ancienneté. Il est régulièrement mis à jour et complété, mais il est attendu que tout le monde y participe.

Arnaud Pince

Venons-en maintenant aux recommandations en matière de sécurité des paiements SEPA (virements et prélèvements). Dans son rapport 2023, l'OSMP constatait que la fraude avait baissé grâce à l'authentification forte, mais que subsistaient d'autres types de fraudes liées à l'ingénierie sociale, ce qui a conduit l'Observatoire à formuler plusieurs recommandations à destination des PSP, notamment renforcer la prévention et la communication auprès du public face aux techniques d'ingénierie sociale, sensibiliser les utilisateurs sur le fonctionnement des prélèvements et améliorer le partage des données de fraude entre établissements.



La loi Labaronne de novembre 2025 sur le partage des données sur la fraude étant entrée en vigueur, j'imagine que les recommandations qui demeurent pour les PSP sont celles portant sur la prévention et la communication auprès du public.

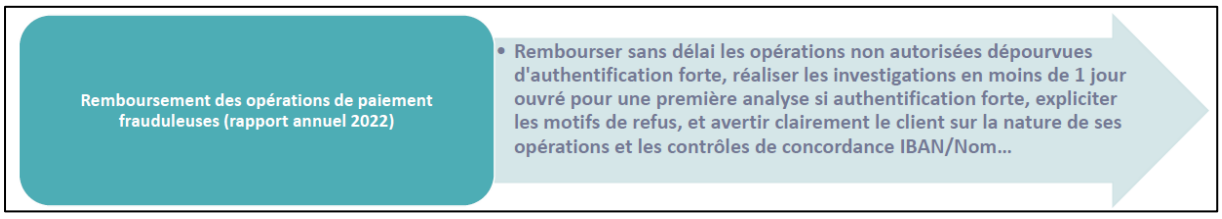
Pierre Bienvenu

Oui. Ce travail de sensibilisation par les PSP est important. Il s'est fait par exemple à propos de l'enregistrement d'un nouveau bénéficiaire de virement. La VoP est venue sécuriser cela, mais il est quand même important de diffuser aux clients les bons messages autour de la confirmation du bénéficiaire.

Parmi les recommandations applicables aux PSP, il y a un point d'attention sur le prélèvement car nous avons le sentiment que les outils de sécurisation (listes noires, listes blanches, possibilité de contester un prélèvement ou de révoquer un mandat…) ne sont pas encore complètement déployés par l'ensemble des PSP. Donc, avec la recommandation de l'OSMP nous remettons en évidence ces dispositions qui figurent dans le Règlement SEPA depuis une dizaine d'années.

Arnaud Pince

Dernier point, les recommandations sur le remboursement des opérations de paiement frauduleuses qui ont été publiées dans le rapport 2022. Là encore, ces travaux de l'OSMP s'inscrivaient dans le contexte de la mise en place de l'authentification forte et notaient le développement de nouvelles formes de fraude, notamment au type ingénierie sociale.



L'OSMP rappelait également la distinction entre opérations autorisées et non autorisées, qui est déterminante pour l'application du régime de remboursement des utilisateurs. L'OSMP recommandait que les PSP encadrent les procédures d'investigation en cas de contestation, avec une première analyse dans un délai de moins d'un jour ouvré et une réponse dans un délai maximum de 30 jours, qu'ils motivent les décisions de refus de remboursement et en informent le client, et qu'ils mettent en œuvre un service de confirmation du bénéficiaire des virements avec une vérification de la concordance entre l'IBAN et le nom du bénéficiaire. Avec l'entrée en vigueur de la VoP, certaines de ces recommandations sont entrées dans le droit.

Pierre Bienvenu

Ces recommandations de l'OSMP ont fait l'objet d'intenses échanges entre tous les acteurs de l'écosystème (les médiateurs, les établissements bancaires, les associations de consommateurs…). Elles sont impératives : il s'agit d'interprétations de la réglementation, mais d'interprétations qui font aujourd'hui consensus.

Nicolas de Sèze

Comme l'a dit Pierre, les travaux ont été extrêmement intenses entre octobre 2022 et mars 2023 et je crois pouvoir dire que les médiateurs ont joué un rôle-clé pour permettre d'aboutir à cet ensemble de recommandations consensuelles, publiées en mai 2023. Rappelons que c'est l'ACPR qui a été chargée d'établir le bilan de la mise en œuvre de ces recommandations, via des enquêtes auprès d'un échantillon représentatif de 14 PSP, bilan dans le rapport 2024 de l'OSMP. On peut enfin souligner que ces recommandations de l'OSMP ont mis la France en bonne position pour inspirer les travaux européens sur la fraude dans le cadre DSP3/RSP.

Hervé Sitruk

Notre échange de ce matin montre que la matière évolue beaucoup, et très vite. Comment prenez-vous en compte ces évolutions ? Faites-vous une actualisation de vos rapports annuels ?

Pierre Bienvenu

Chaque année, nous essayons de rappeler dans le nouveau rapport (cf. section 3.5 du rapport 2024) les principales recommandations, pour éviter au lecteur de devoir aller les rechercher dans les rapports annuels antérieurs. Mais nous recommandons toujours la lecture de l'étude dans son ensemble pour avoir les éléments de contexte. Il nous semble que l'essentiel des recommandations restent valables, même si certaines ont pu, dans l'intervalle, être incorporées dans la réglementation. Mais peut-être serons-nous amenés à faire du nettoyage sur les études les plus anciennes et à supprimer certaines références dans l'annexe au RACI.

Cathie-Rosalie Joly

Nous évoquions précédemment des mesures de prévention sur la fraude pour les paiements à distance hors 3D Secure. Ce sont des recommandations de 2023 qui ont fait l'objet d'une mise à jour en janvier 2026. Appliquerez-vous la même démarche de mise à jour pour d'autres recommandations ?

Pierre Bienvenu

La mise à jour de janvier 2026 était plutôt cosmétique, mais plus généralement, à travers l'annexe du RACI, notre message principal est que la publication du rapport de l'Observatoire doit être chaque année un moment fort pour les PSP, et qu'il faut prendre connaissance du rapport.

Marie-Agnès Nicolet

C’est aussi aux PSP de regarder ce qui est applicable, ce qui a fait l'objet de réglementations ultérieures ?

Pierre Bienvenu

Nous sommes dans une logique de sensibilisation et de dialogue avec les PSP. Nous leur rappelons les recommandations passées qui nous semblent largement valables. Certaines sont impératives (par exemple celles, évoquées plus haut, portant sur le remboursement des opérations de paiement frauduleuses, ou sur le prélèvement), mais pour celles qui sont plutôt de l’ordre des bonnes pratiques, nous pouvons tout à fait admettre qu’un PSP fasse état, en toute transparente vis-à-vis de la Banque de France, d’une conformité seulement partielle (par exemple sur la préparation à l’informatique quantique).

Cathie-Rosalie Joly

Parmi les sujets qui vont occuper l'année 2026, vous avez évoqué l'IA et le règlement eIDAS. Y a-t-il d’autres sujets ? Je pose la question parce que FRANCE PAYMENTS FORUM, via ses groupes de travail, aurait certainement des retours à partager avec l'OSMP.

Pierre Bienvenu

Je réalise que dans l’annexe du RACI 2025 nous avons omis de mentionner l’étude sur l’IA que nous avons publiée dans le rapport 2024 de l’OSMP (avec une recommandation en matière de backtesting). Nous l’introduirons dans la prochaine édition. Dans le rapport OSMP de cette année, nous allons publier une étude de veille sur la sécurité des paiements par crypto-actifs. Et nous venons de lancer des études sur les nouvelles solutions d'authentification, les paiements agentiques et l'identité numérique. Nous commençons tout juste et je ne sais pas encore comment cela va atterrir, mais l'objectif c'est d'apporter un éclairage à l'écosystème sur ces sujets complexes et extrêmement mouvants, avec des recommandations qui soient autant que possible le fruit d’un consensus.

Hervé Sitruk

Je voudrais remercier les intervenants et inviter ceux des participants qui ne sont pas encore membres à rejoindre FRANCE PAYMENTS FORUM. Nous sommes une association d'experts et de professionnels des paiements. Nous avons une dizaine de groupes de travail. Nous organisons le 12 mars une Rencontre digitale sur l'urgence des stablecoins. Nous en organiserons prochainement une autre sur l'identité numérique et une autre sur le panorama des réglementations applicables aux paiements. Le 16 mars, notre GT EWPF organise comme chaque année une Rencontre en présentiel dans le cadre de la journée internationale des femmes. Et le 14 avril, nous organisons une grande rencontre, également en présentiel, sur la souveraineté dans les paiements. Merci à tous.