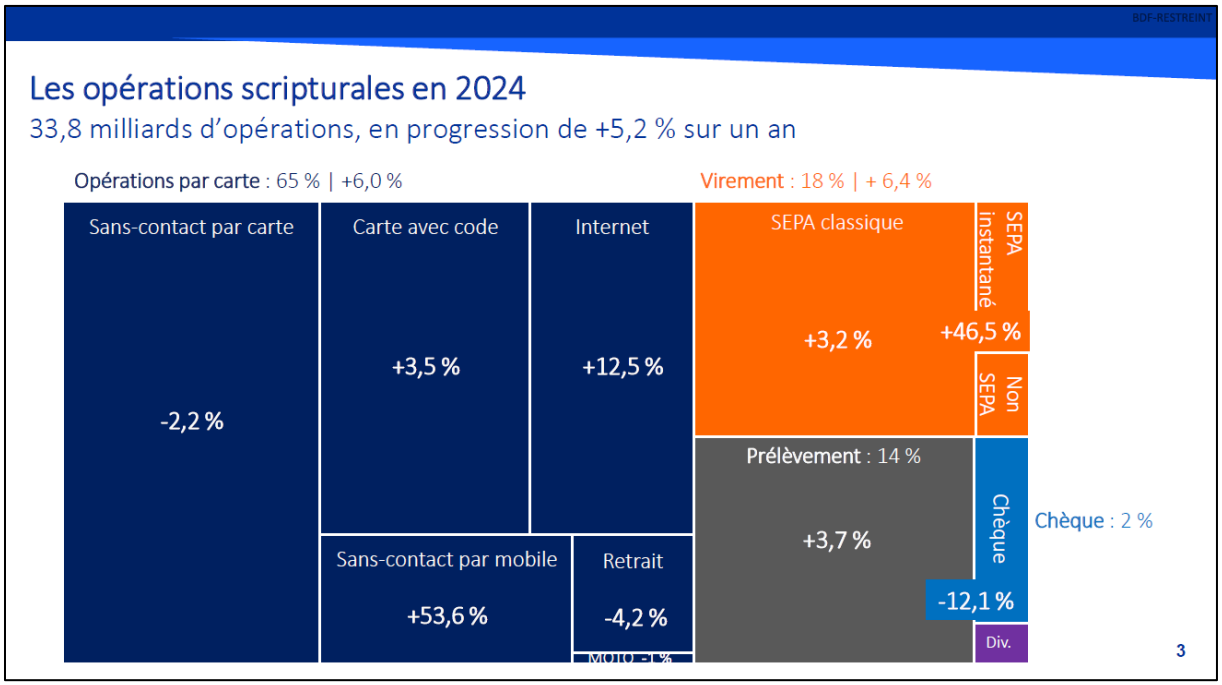
# FRANCE PAYMENTS FORUM

## Rencontre digitale du 25 septembre 2025

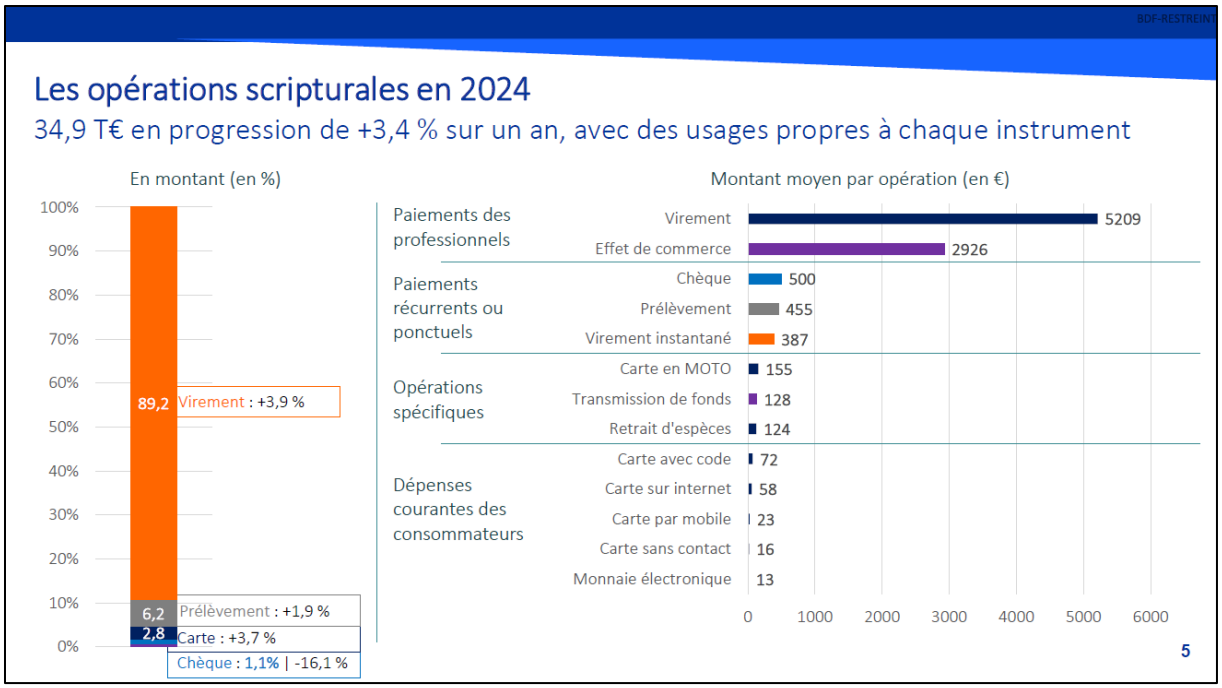
## Intervention de Julien Lasalle

## *Les enseignements du 9ème rapport annuel de l'OSMP*

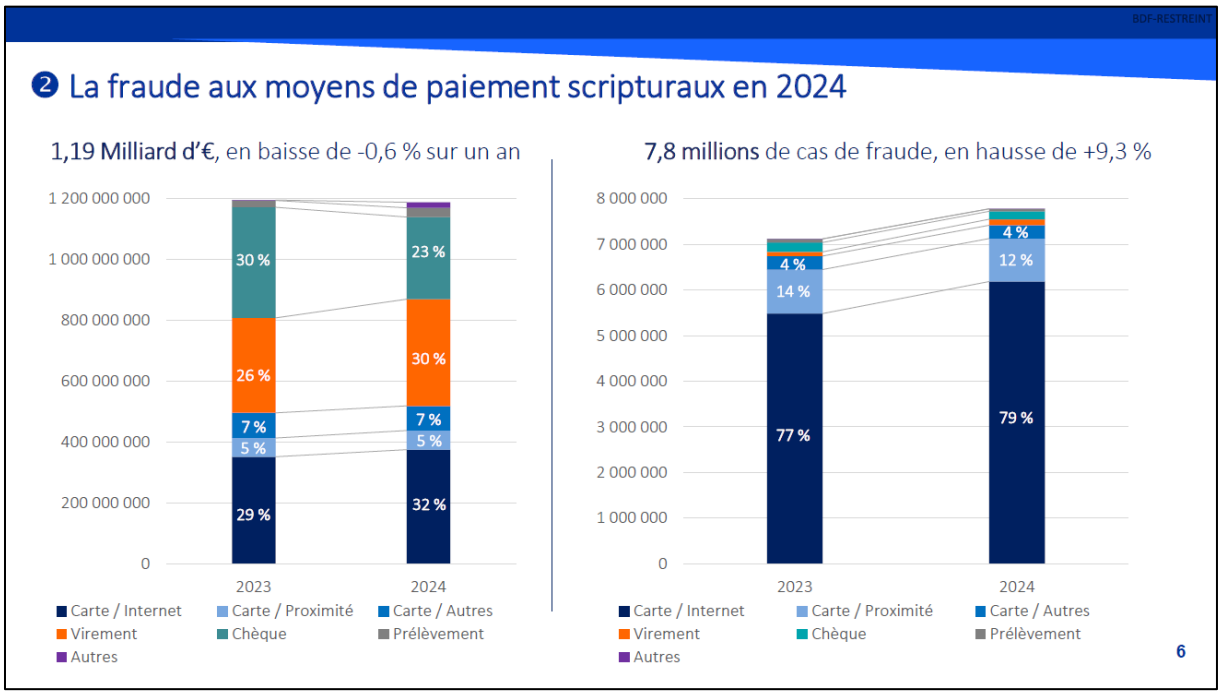
Le rapport 2024 de l'OSMP a été publié le 9 septembre. Comme toujours, il commence par les statistiques annuelles sur les paiements et la fraude, ce « thermomètre » qui guide notre action. Le chapitre 2 porte sur le bilan des recommandations adoptées par l'OSMP en mai 2023 sur le remboursement des opérations frauduleuses. Le chapitre 3 est consacré au suivi des actions de prévention de la fraude conduites par l'Observatoire. Le chapitre 4 porte sur les travaux de veille technologique de l'OSMP qui, cette fois, ont été consacrés à l'intelligence artificielle, sujet sur lequel la Banque de France a d'ailleurs organisé une conférence le 6 mai dernier afin de présenter la teneur de ces travaux.



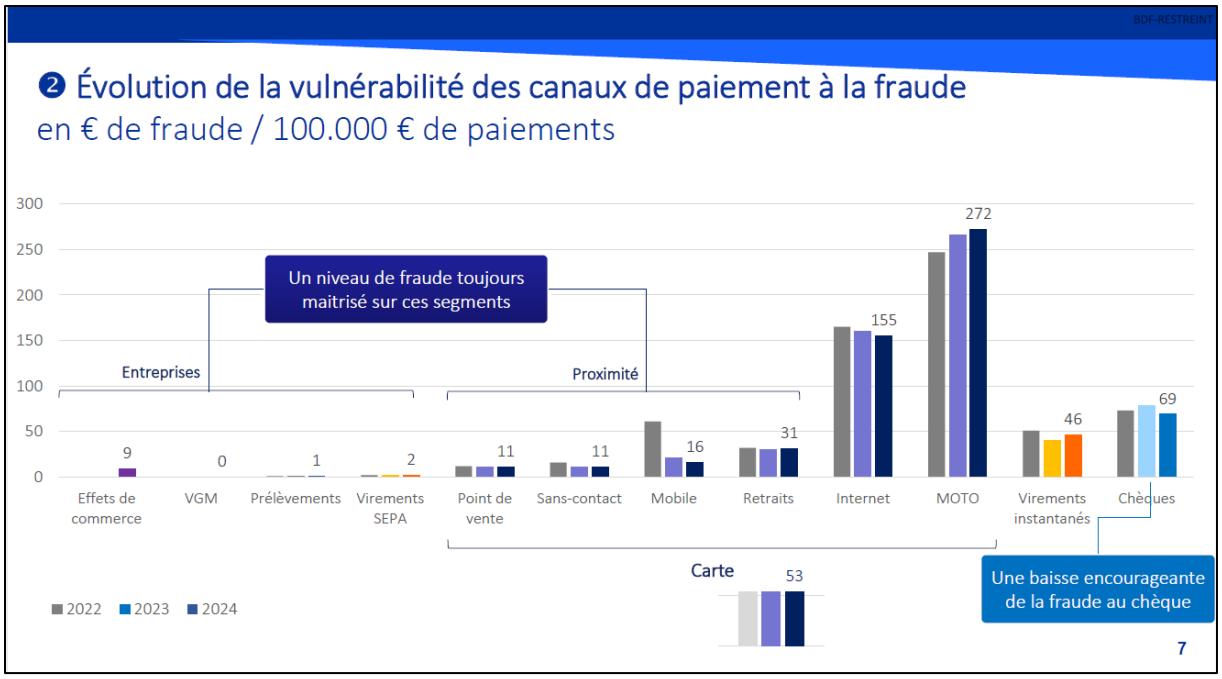

Le marché des paiements continue de progresser, avec une hausse de 5,2% en volume, tirée par des deux « locomotives » qui sont la carte et le virement, alors que le chèque a vu son usage continuer à diminuer, et ne représente plus que 2% du nombre de transactions scripturales. La carte reste un instrument majoritairement de proximité, même si on a quand même 19% des opérations sur internet, et parmi ces opérations de proximité, 68% sont en sans contact, dont 15% par mobile. Il s'agit des chiffres de 2024, et il est très probable qu'en 2025 les parts relatives des paiements mobiles et du virement instantané (à la faveur du déploiement de Wero) seront sensiblement plus élevées en 2025.




En valeur la progression est un peu plus modeste (+3,4%), et c'est toujours le virement qui représente la plus grande part des flux de paiements en valeur (89,2%) : ce sont les paiements des entreprises, des administrations.




En valeur, la fraude est restée stable en 2024, à 1,2 milliard, mais sa répartition évolue : la part du chèque est tombée de 30% à 23% alors que celle du virement passait de 26% à 30% et celle de la carte de 29% à 32%. En nombre, les cas de fraude sont en hausse de +9,3%. Ceci signifie que les fraudeurs font plus de transactions frauduleuses mais de moindre montant, autrement dit « tentent leur chance » un plus grand nombre de fois sur des plus petits montants.




Les taux de fraude les plus bas sont ceux du segment entreprises et du segment des paiements de proximité par carte et ils sont très stables dans le temps.

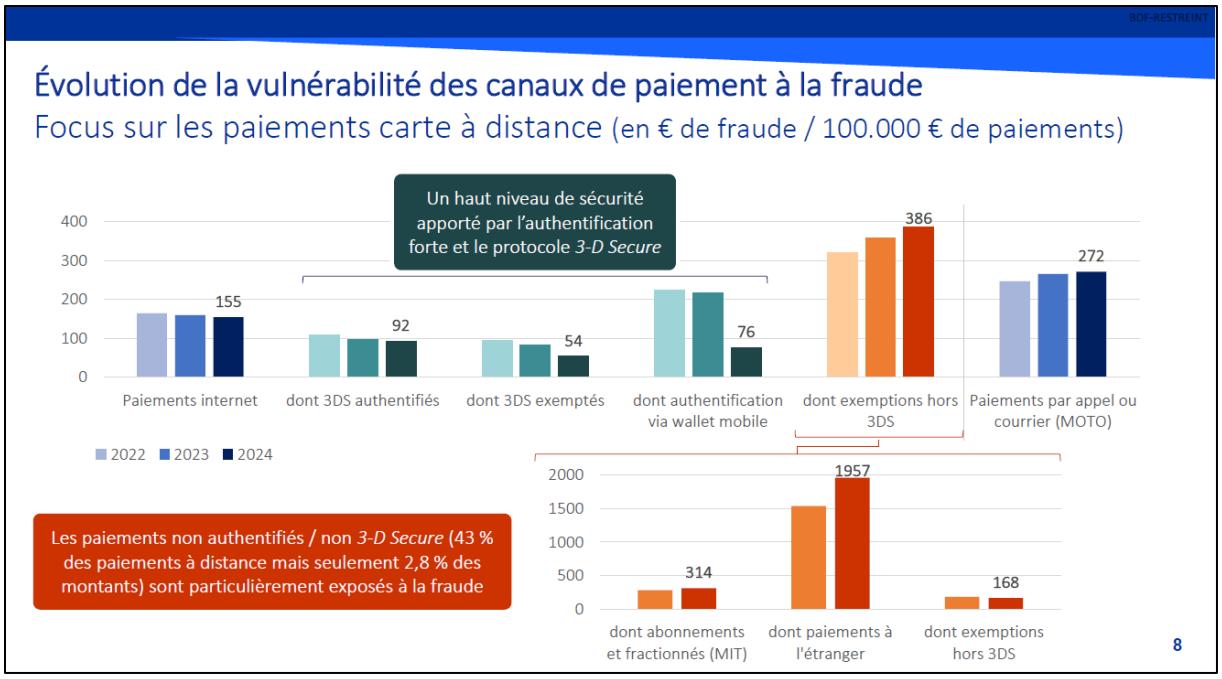
Le taux de fraude du paiement par mobile qui, depuis deux ans, est rentré dans le rang, se rapproche du taux de fraude moyen du sans contact, ce qui est rassurant.

En revanche, le paiement carte sur internet reste proportionnellement « surfraudé » avec un taux de fraude trois fois supérieur au taux de fraude moyen, mais qui baisse grâce à l'effet de la DSP2, de l'authentification forte ou du scoring. Mais dans l'autre sens, le paiement MOTO, qui représente des masses de paiement de plus en plus faibles, a un taux de fraude qui continue à croître. J'y reviendrai plus loin.

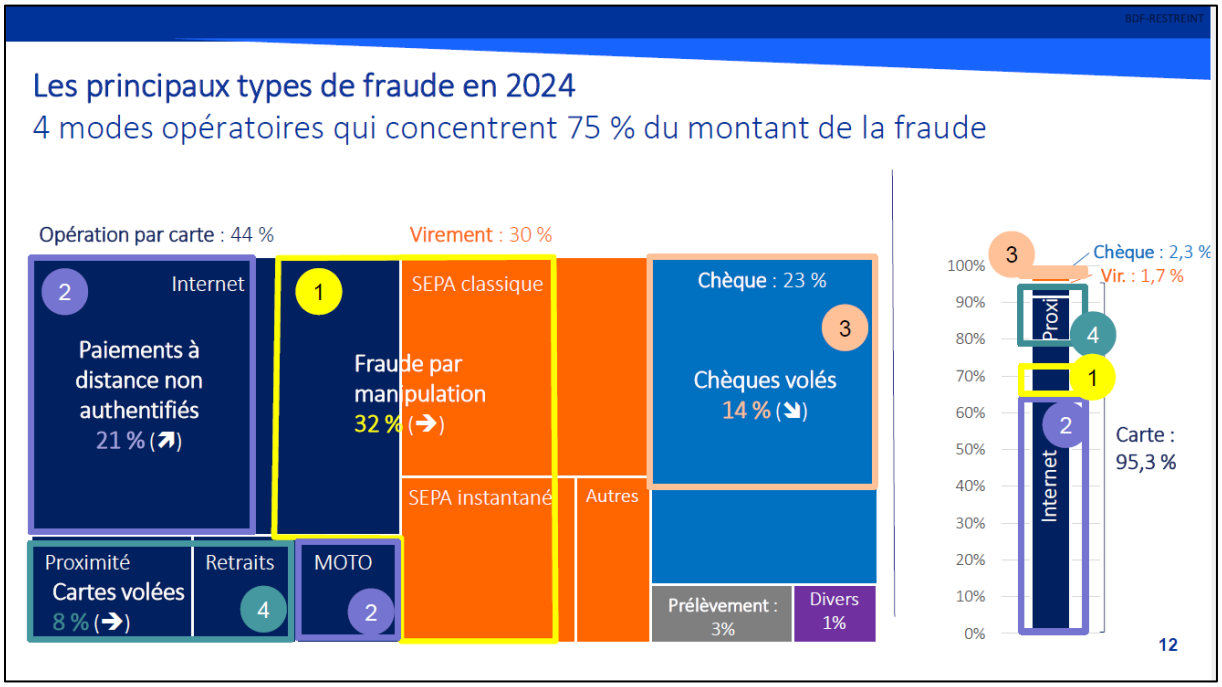
Sur le chèque, depuis la mise en place du plan d'action de l'Observatoire, le taux de fraude est reparti à la baisse, ce qui est encourageant.

Le virement instantané a un taux de fraude qui oscille aujourd'hui autour des 45 euros de fraude pour 100 000 euros de paiement. Nous n'avons pas de grosse inquiétude sur la légère progression observée l'an dernier e dernière, et on note que ce taux de fraude est inférieur à celui des paiements par carte sur Internet qui, en termes d'outils de sécurisation, sont ceux qui se rapprochent le plus de l'usage aujourd'hui du virement instantané.

Sur les paiements sur Internet, nous sommes capables de faire tout un découpage des protocoles, modes d'authentification qui sont utilisés, et ceci montre que quand on utilise 3D Secure, que ce soit pour authentifier le paiement ou pour l'exempter, ou bien quand on utilise un wallet mobile avec une authentification de type Apple Pay ou Google Pay qui permet de faire un paiement Internet authentifié (même si ce n'est pas dans 3D Secure), on a des taux de fraude très bas et qui continuent à baisser, ce qui est, là aussi, rassurant.




En revanche, tout le reste, c'est-à-dire les exemptions 3D Secure, les MIT, les paiements à l'étranger, présentent des taux de fraude structurellement très élevés. Et même les exemptions hors 3D Secure sont sur-fraudées par rapport aux exemptions dans 3D Secure. Cela nous montre quels sont les segments auxquels nous devons nous intéresser aujourd'hui.




Concernant la répartition en valeur de la fraude, on voit que **quatre modes opératoires** concentrent 75% du montant total de la fraude.

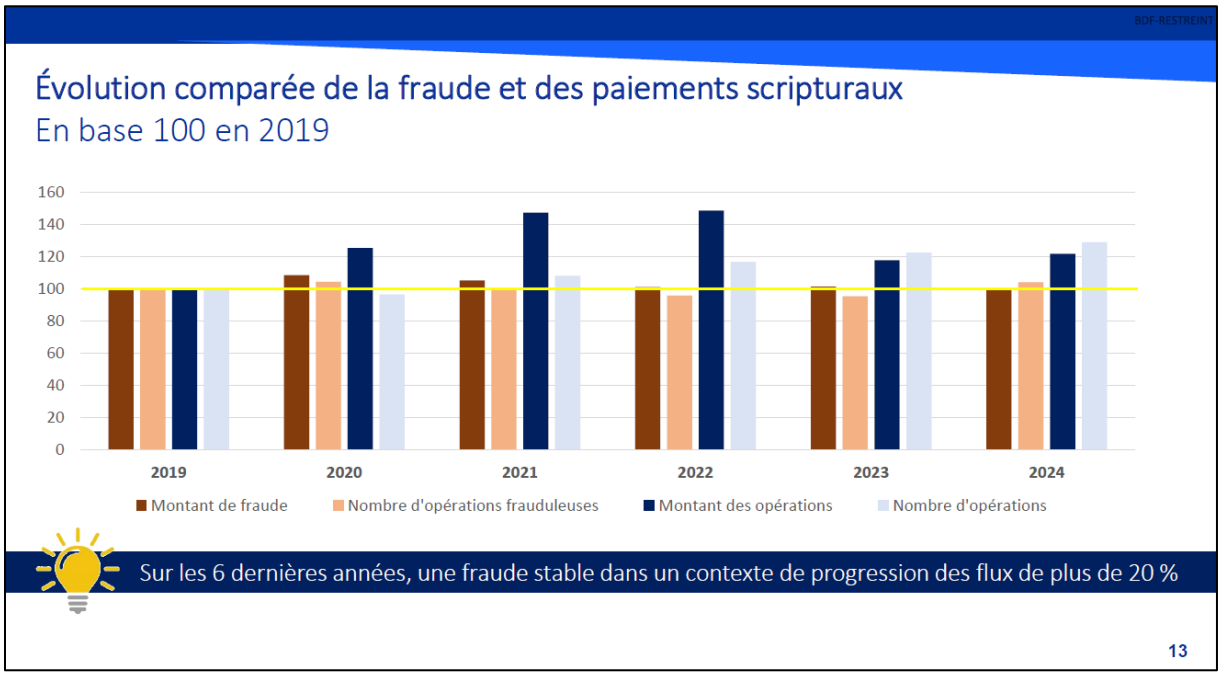
Le premier est la **fraude par manipulation** : fraude au conseiller bancaire, fraude au président dans les entreprises, usurpation de coordonnées bancaires, substitution d'IBAN dans les factures… en bref, ce que les anglais appellent les Authorized *Push Payments* (ADP). Ils

représentaient en 2024 un montant de fraude d'environ 380 millions d'euros, montant qui s'est arrêté de progresser cette année alors que depuis le passage à la DSP2, il avait progressé de façon continue . Cette stabilisation est pour nous un signe que les actions que nous avons entreprises (j'y reviendrai plus loin) commencent peut-être à porter leurs fruits.

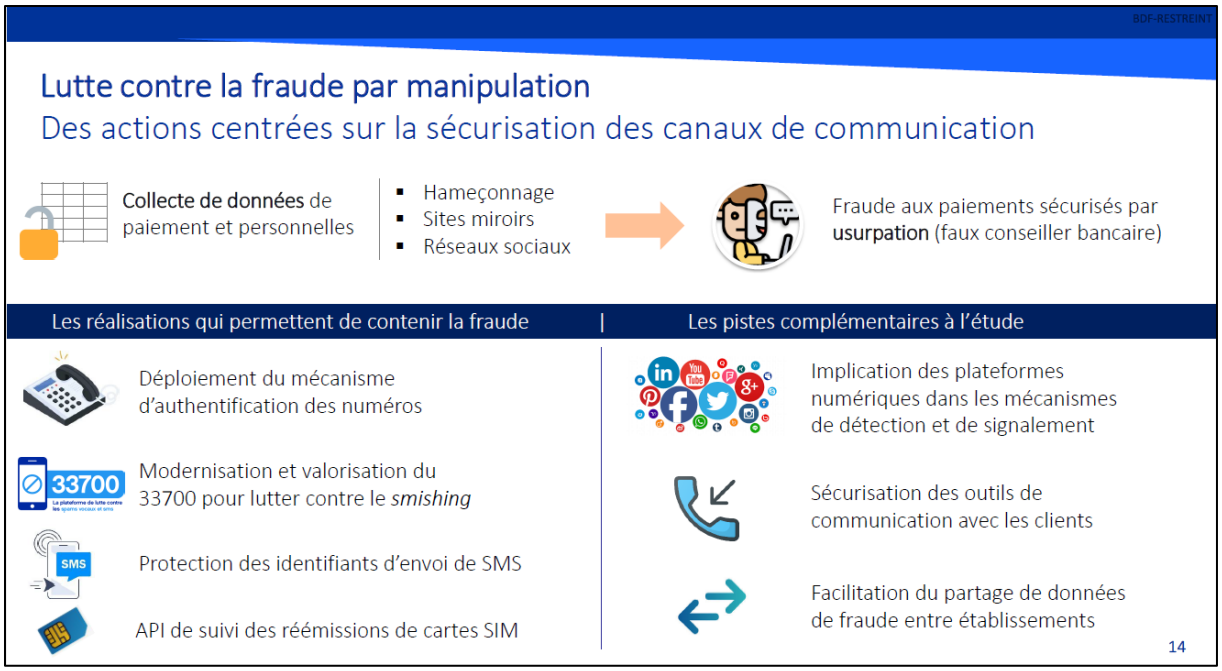
Le deuxième sont les **paiements à distance non authentifiés**, c'est-à-dire les MOTO, les MIT, les paiements cross-border hors union européenne. C'est là que nous avons la plus grosse proportion de transactions frauduleuses : des petites transactions, mais très nombreuses. Nous soupçonnons toutefois que dans cette catégorie il y ait de toutes petites transactions classées par défaut dans la fraude et dont le montant ne justifie pas de faire des travaux pour savoir s'il ne faudrait pas les qualifier en litige commercial, ce qui vient sans doute un peu polluer nos statistiques.

Le troisième est sur **le chèque :** chèques perdus ou volés, notamment dans les circuits de distribution, qui représentent quand même au total 14% de la fraude chiffre en baisse mais qui suit en fait le mouvement à la baisse de l'utilisation du chèque.

Le quatrième, sur lequel nous ne travaillons pas vraiment, ce sont les cartes volées, avec ou sans code confidentiel, qui génèrent un petit « bruit de fond » en termes de fraude, mais avec des taux de fraude qui sont tout à fait acceptables(0,010%). C'est un instrument très bien sécurisé avec le *CHIP and PIN* et les mécanismes de protection du sans contact.




La bonne nouvelle est que depuis 2019, le montant et le nombre des opérations frauduleuses sont stables alors que pendant le même temps les flux en valeur ont progressé de plus de 20% et le nombre d'opérations de quasiment 30%.




Les actions de l'Observatoire sont centrées sur les trois grands segments sur lesquels il y a le plus de fraude.

**Sur la fraude par manipulation**, nos actions ont porté sur la sécurisation des parcours de paiement, mais aussi sur les travaux avec les opérateurs de téléphonie : nous avons suivi le déploiement du mécanisme d'authentification des numéros, et travaillé sur la sécurisation des envois de sms, la lutte contre le smishing, et contre le SIM swapping. Le plus gros du travail que nous pouvions espérer faire avec les opérateurs de téléphonie a été fait, et il faut attendre que tout cela produise des effets : l'authentification des numéros est opérationnelle depuis le début de cette année,  donc par définition ce n'est pas dans les chiffres 2024.

Aujourd'hui, le sujet est de voir comment nous pourrions travailler avec les opérateurs de plateformes numériques pour partager avec eux les mécanismes de détection et de signalement. Par exemple, sur votre iPhone vous pouvez supprimer un SMS et le signaler comme frauduleux, mais on ne sait pas ce que devient cette information (en tout cas elle n'est pas partagée avec les opérateurs). Elle permet donc peut-être de protéger d'autres utilisateurs d'iPhone, mais pas de protéger l'ensemble de la population. Il faut donc comment on pourrait faire interagir ces mécanismes de signalement, par exemple, avec le 33 700.

Nous avons aussi la question de la sécurisation des outils de communication avec les clients, pour filtrer les fausses communications ou fausses publicités que l'on voit beaucoup sur les réseaux sociaux, sou même sur des sites officiels.

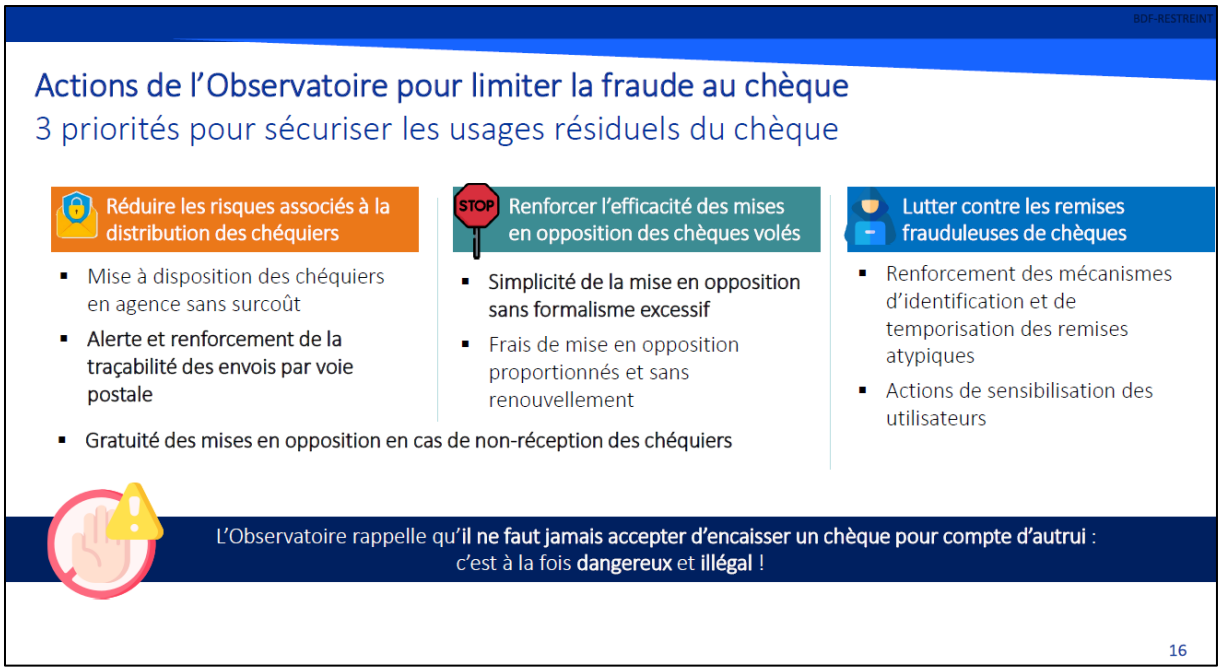
Dernier point : le partage de données entre établissements : les IBAN frauduleux, la VoP …sont des outils qui devraient permettre de lutter contre certains types de fraude par manipulation.

Concernant les paiements par carte à distance non sécurisés, nous avons **trois cibles** : les MOTO, les MIT et les « *direct to authorization* », c'est-à-dire les exemptions hors 3D Secure. Nous avons une approche par seuils et par limitation de ces paiements. Nous avons demandé aux émetteurs de rejeter les transactions dès lors qu'elles excèdent un certain niveau par commerçant, par jour, par client avec des exemptions parce que certains secteurs sont par exemple dépendants des MOTO. Nous avons ciblé les dix commerçants les plus exposés à la fraude sur les MIT et sur les MOTO, pour dialoguer avec eux sur ce qu'on pourrait faire pour sécuriser leurs flux.

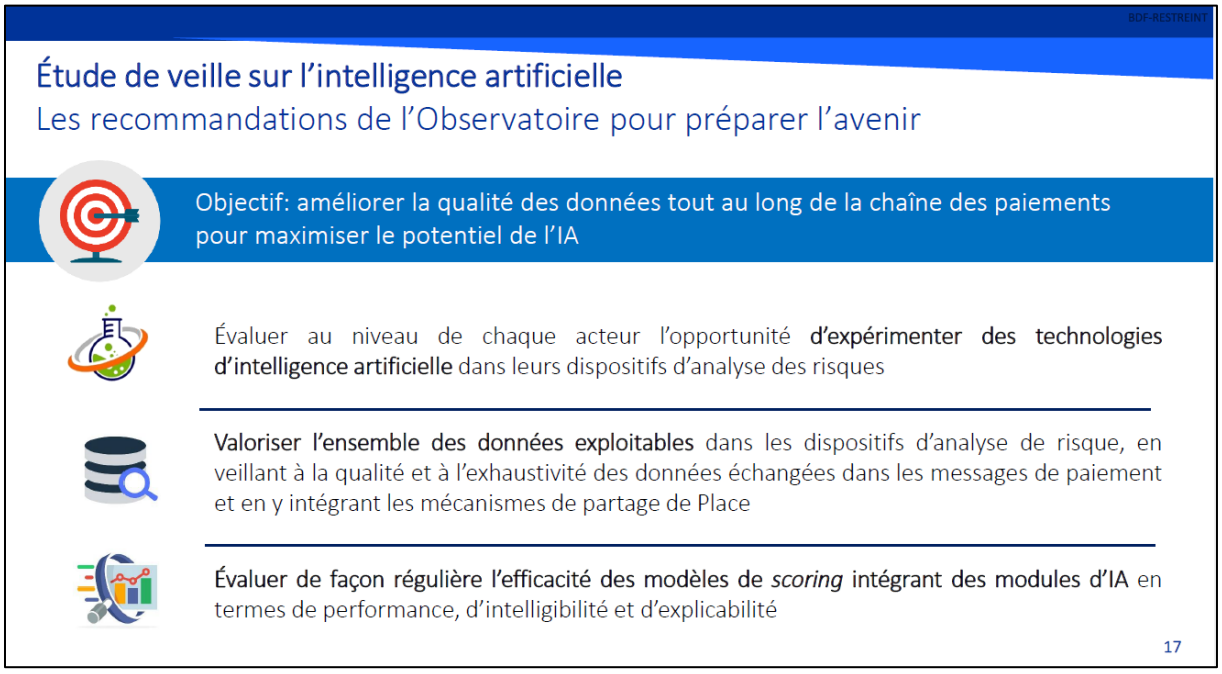
Nous allons poursuivre et accentuer cette logique, pour faire en sorte que les commerçants n'utilisent pas à tort ces canaux de paiement du genre « je vends sur internet, je vois que mon client n'arrive pas à s'authentifier, je transforme le paiement MOTO, et passe tout seul ». or c'est interdit et nous allons donc faire la chasse à ces pratiques.

Notre logique de seuils sera un peu plus étalée dans le temps, car nous avons conscience que cela pose des difficultés.  Nous allons donc travailler avec les commerçants concernés pour leur permettre de s'y préparer, et nous n'excluons pas de regarder la possibilité d'appliquer cela aux flux internationaux. En effet, sachant que certaines zones géographiques sont prêtes pour 3D Secure et l'utilisent sur leurs transactions domestiques, on ne comprend pas qu'ils ne l'utilisent pas sur des flux cross-border qui impliquent une carte française. Nous allons donc cibler notre approche en fonction du degré de maturité et du degré de fraude que l'on observe dans les autres zones géographiques.

Nous continuons à soutenir l'émergence de solutions d'authentification sur certains segments tes que les *telephone orders (TO).* Et puis, il y a un impératif d'assurer une traçabilité des mandats de MIT, car aujourd'hui les authentifications à 1 euro ou à 0 euro ne servent à rien et ne permettent pas aux établissements de faire le tri dans les flux qu'ils reçoivent.




Sur le chèque, nous poursuivons le plan d'action, la principale difficulté étant aujourd'hui les circuits de distribution des chéquiers. Nous avons pris des résolutions fortes pour inviter les établissements à mieux suivre, à mieux alerter leurs clients lorsqu'ils leur envoient des chéquiers, avec des *reminders* pour qu'en cas de non-réception la mise en opposition soit rapide. Le corollaire est que les frais de mise en opposition doivent être proportionnés, car les clients préfèrent ne pas mettre en opposition si cela leur coûte cher. Il va de soi, mais nous l'avons rappelé, que par définition un chéquier non reçu ne peut pas faire l'objet de frais de mise en opposition parce que le client ne l'a pas eu entre les mains.




Sur l'IA, nous avons eu cette belle conférence du 6 mai dernier. Je ne vais pas vous présenter

l'étude, mais vous savez comme moi que l'IA apporte de formidables capacités de scoring et d'exploitation des données, mais aussi que d'autres types d'IA, notamment générative, sont entre les mains des fraudeurs pour générer des campagnes de phishing, y compris en multi-langues, pour créer des faux sites miroirs de commerçants, d'administrations, de banques.

La mise en place du cadre DSP2 a entraîné cette course en avant sur la guerre **IA** contre IA, avec d'un côté les protecteurs des paiements qui vont utiliser l'IA pour mieux détecter les risques et de l'autre les attaquants qui vont utiliser d'autres capacité de l'IA pour multiplier leurs attaques et les rendre plus crédibles.

l'Observatoire a formulé trois recommandations.

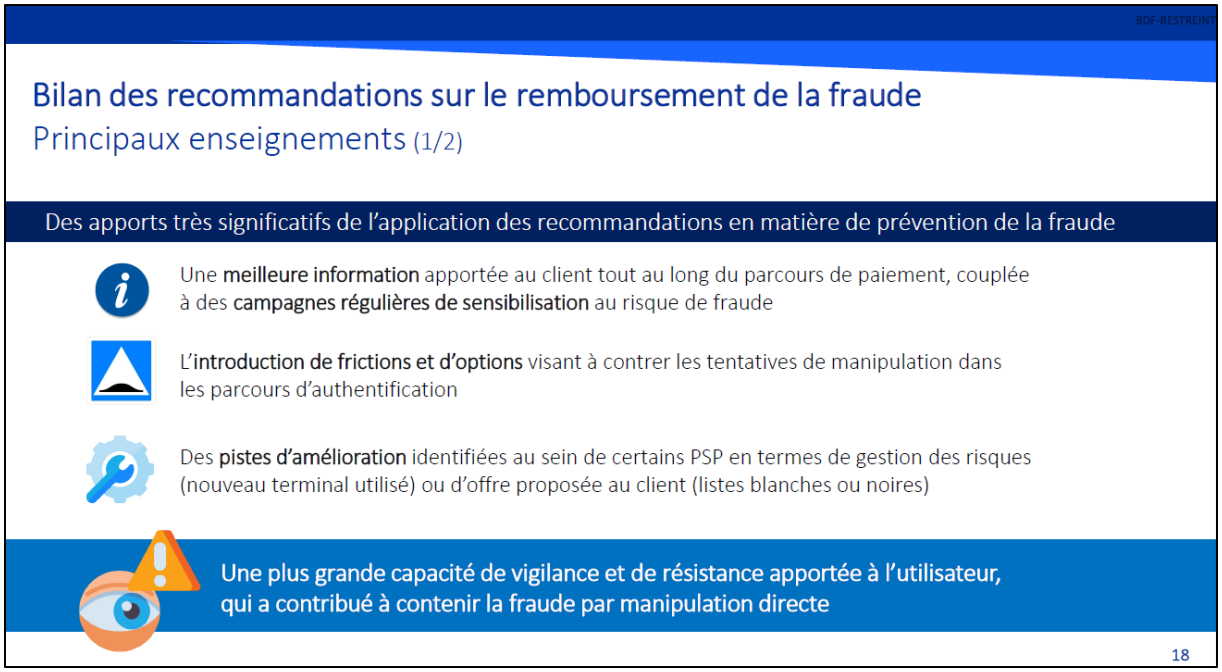
- Inviter les acteurs de la chaîne des paiements à expérimenter les technologies d'IA pour continuer à faire évoluer leur mécanisme d'analyse des risques. Cela vaut bien sûr pour les banques, les *schemes* et les systèmes, mais aussi pour les commerçants. On sait que certains grands commerçants sont très efficaces sur l'utilisation de ce genre d'outils.
- Veiller à la qualité des données. Par exemple, un commerçant qui remplit des champs dans 3D Secure V2 car il veut demander une exemption, doit le faire proprement, sinon les données ne sont pas exploitables par les outils de scoring des banques ou des *schemes*. Il est donc important que chaque acteur qui, à un moment du cycle de paiement, injecte des données qui peuvent être utilisées à des fins de lutte contre la fraude, soit vigilant sur la qualité et la complétude de ces données.
- Être capable d'expliquer les résultats que fournissent les moteurs d'IA, sans forcément avoir à comprendre comment fonctionne l'algorithme, mais en étant capable de lire et de comprendre les résultats qui sont fournis, puis de mesurer l'efficacité a posteriori, donc faire du *backtesting,* et se dire qu'il faut rester en mouvement sur ce type de technologie et faire évoluer les moteurs car à partir du moment où les moteurs de scoring deviennent statiques, les fraudeurs arrivent à identifier leurs paramètres.

Dernier point que je souhaite vous présenter, car c'est un sujet nouveau dans le rapport de cette année : nous avons dressé, avec l'ACPR, un **bilan de la mise en œuvre des recommandations OSMP de mai 2023 sur le remboursement des cas de fraude**. Nous en tirons deux enseignements.

**Sur le volet prévention de la fraude,** des progrès très significatifs ont été accomplis en la matière, avec des parcours clients beaucoup plus explicites et mieux maîtrisés par les utilisateurs. Il y a aussi de belles campagnes de sensibilisation, collectives et individuelles.

Il y a même eu des choix d'introduire des frictions et des options qui permettent globalement de contrer les tentatives de manipulation, permettant en quelque sorte d'avoir une corde de rappel sur l'utilisateur quand, dans son parcours client, il est sous l'emprise d'un fraudeur. Par exemple, lui poser la question « êtes-vous en ligne avec votre conseiller bancaire ? », ou bien avoir des fenêtres d'authentification qui permettent non seulement de valider le paiement mais aussi de le rejeter, ce qui n'était pas toujours le cas jusqu'à présent.

Il y a encore des pistes d'amélioration chez certains PSP, par exemple la gestion des risques en cas de nouveau terminal, ou bien les listes blanches ou listes noires sur les prélèvements mais, globalement, la capacité de vigilance et de résistance apportée à l'utilisateur a réellement augmenté et c'est une des raisons de l'inversion de la courbe de la fraude par manipulation.




**Concernant le volet traitement des réclamations**, sur lequel l'OSMP avait émis des exigences fortes, nous considérons qu'il est aujourd'hui conforme à l'esprit des recommandations, c'est-à-dire la prise en compte par les banques des critères recommandés par l'OSMP (paramètres d'émission de la transaction, bon fonctionnement des outils d'authentification, contexte de l'opération…) avant de se prononcer.

Nous avons noté que les établissements ont abandonné certaines exigences, telles que la remise de documents signés ou d'un dépôt de plainte.

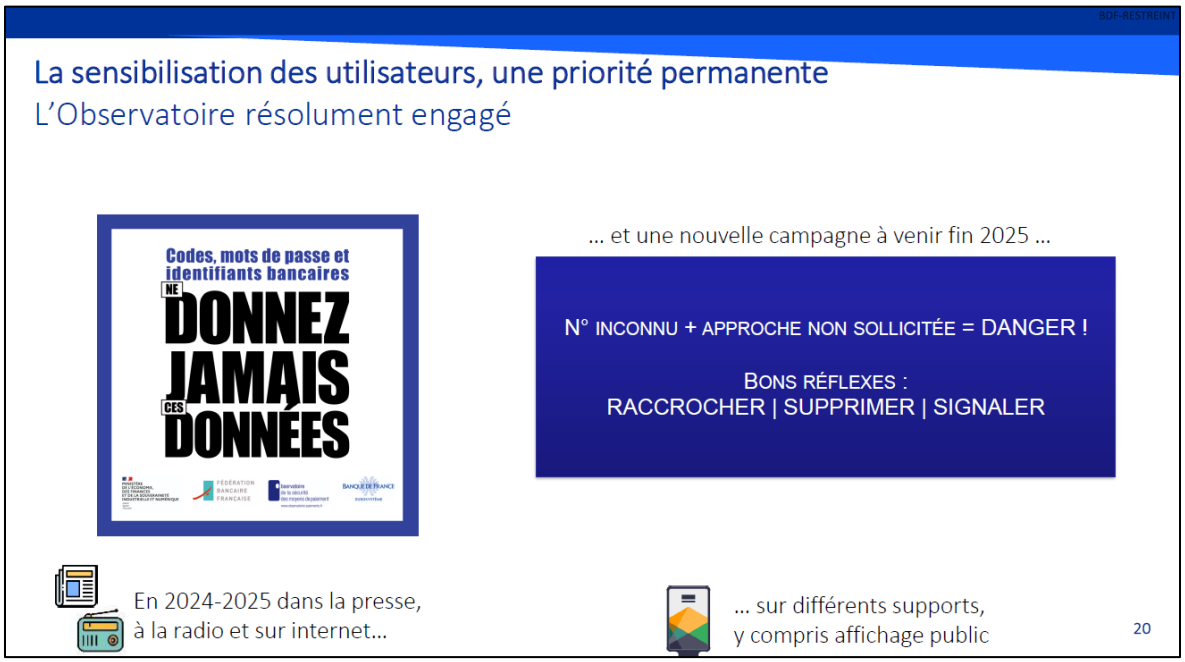
Des progrès sont encore attendus, en particulier sur la restitution faite au client par le PSP quand il refuse de rembourse. Par exemple si le PSP invoque la négligence grave, il doit être en mesure de fournir des traces techniques, même s'il considère que le client n'est pas à même de les comprendre, car le client peut se faire accompagner.

Notre préoccupation n'est pas d'avoir un taux de remboursement cible (sauf sur certains cas particuliers), mais d'avoir une hiérarchie des taux de remboursement cohérente avec le traitement qui est réalisé. Globalement, c'est bien le cas, et nous notons que dans les contestations il y a aussi des cas de litiges commerciaux et de contestations abusives, qui représenterait environ 25% des réclamations.

Le point qui nous pose encore des difficultés est celui des virements sans authentification forte. S'il n'a pas d'authentification forte, cela veut dire qu'il n'y a pas de trace de l'autorisation, donc les virements devraient être remboursé à 100%, comme c'est le cas pour les cartes. Aujourd'hui, sur les paiements par carte sans authentification forte, on a un taux de remboursement de 98% qui nous semble conforme à l'esprit de la réglementation.

Et renforçant les parcours d'authentification, on a aussi donné des outils d'analyse aux banques, qui sont en mesure de démontrer, traces informatiques à l'appui, que le client a validé telle et telle chose, qu'on lui a posé telle question en cours de route et qu'il est passé outre. Les banques peuvent donc aussi utiliser le renforcement des parcours client comme des éléments d'instruction de leur dossier de réclamation. C'est pour cela qu'il nous importe de nous assurer que la hiérarchie globale des taux de remboursement est cohérent. Ce sont donc des indicateurs que nous allons continuer de suivre dans la durée, aux côtés de l'ACPR.

Un dernier mot pour dire que l'OSMP est très engagé sur les **actions de sensibilisation**.



L'OSMP s'était associé notamment à la FBF et à Bercy en 2024 et 2025 dans des campagnes de sensibilisation sur le thème « Ne donnez jamais aux données » .

La nouvelle campagne qui sera lancée d'ici un mois et demi visera plutôt les supports de type affichage public, qui permettent d'avoir un impact client assez large (c'est ce que nous disent les communicants) sur des messages complémentaires tels que « quand vous avez un appel ou un message d'un expéditeur inconnu et non sollicité, c'est a priori une situation potentiellement dangereuse et il y a quelques réflexes à adopter : raccrocher, supprimer ou signalés, selon les situations.

Merci de votre attention.

***

## Questions-réponses

### Hervé Sitruk

*Merci beaucoup Julien. Ta présentation a bien montré les progrès que l'OSMP a fait faire dans la lutte contre la fraude, en ayant une vision de place et non pas par système. Tout à l'heure, nous avons évoqué avec Éric Ducoulombier l'objectif de porter au niveau européen un équivalent de l'OSMP, ainsi que le débat, dans le cadre de la négociation sur la future DSP, sur l'inclusion des acteurs technologiques dans la lutte contre la fraude aux paiements. Peux-tu nous en dire quelques mots ?*

### Julien Lasalle

Comme vous le savez, au niveau national nous avons fait évoluer les textes qui régissent la composition de l'OSMP afin de pouvoir inclure les telcos. Nous allons tendre la main aux réseaux sociaux, toujours dans une logique de volontariat et de partenariat car la Banque de France n'a aucun pouvoir pour imposer quoi que ce soit à Meta ou à Google. En revanche, nous sommes sensibles au fait que des initiatives de coopération existent ailleurs, par exemple au Royaume-Uni, et nous voulons sensibiliser ces acteurs et voir dans quelle mesure nous pouvons les associer à nos travaux.

Le problème est qu'une réglementation européenne sur les paiements ne peut pas embarquer n'importe quelle catégorie d'acteurs qui ne relèvent pas nativement du champ des paiements. Il faut donc voir s'il est possible de s'appuyer sur des textes européens tels que le DSA pour assujettir ces acteurs-là à des exigences relatives à la lutte contre la fraude, sans pour autant en faire des assujettis au sens de la supervision bancaire ou des paiements (ce qui n'aurait aucun sens).

Mais au niveau national, le cadre de l'OSMP nous permet de prendre contact avec des acteurs qui ne sont pas membres de l'Observatoire et de les impliquer dans nos travaux. Nous voulons donc saisir à fond cette opportunité.

## Hervé Sitruk

*On dit classiquement que pour qu'il y ait sécurité, il faut qu'il y ait identification, authentification, intégrité, non-répudiation, et non-révocabilité.*

*Sur l'authentification, il y a eu des progrès de l'authentification forte.*

*Sur l'identification, avec la perspective d'entrée en vigueur d'eIDAS2 en 2027, la question est la possibilité d'appliquer eIDAS2 dans le monde des paiements. Il serait bon que l'OSMP se penche sur ce sujet, car on voit qu'en Europe il y a beaucoup d'initiatives, y compris dans le monde des paiements, et que beaucoup de questions qui se posent. Nous avons des experts, mais il faut que l'OSMP prenne le leadership. Nous savons que des acteurs non-européens vont proposer des solutions qui n'auront pas de logique eIDAS2 mais qui auront des compatibilités techniques et qui vont essayer de prendre des parts de marché. Et tout à l'heure Laetitia Dorla nous a indiqué que Wero va aussi essayer d'avancer sur ces questions-là.*

*Sur l'intégrité : pour qu'il y ait intégrité, il faut que le message soit sécurisé de bout en bout. Et aujourd'hui, on n'y est pas.*

## Julien Lasalle

Concernant **l'identité numérique**, je rappelle que l'OSMP y a consacré une belle étude de veille dans son rapport 2021[1]. Nous avons toujours vu l'identité numérique comme quelque chose qui peut apporter de la confiance et de la sécurité au secteur des paiements. Par exemple, en sécurisant l'entrée en relation, en permettant d'apporter des couches de sécurité. Nous sommes très attentifs à ce qui se passe, et nous n'excluons pas de lancer une actualisation de notre étude.

Ce qui nous rassure, c'est de voir que des acteurs du monde des paiements (b.connect, Wero) commencent à réfléchir à embarquer des fonctionnalités qui sont celles du service d'identité numérique en s'appuyant sur les technologies du monde des paiements. Donc, d'une certaine manière, la complémentarité entre identité numérique et paiement est en train de s'établir, y compris au sein des acteurs du monde des paiements, et c'est une très bonne chose.

Concernant **l'intégrité**, nous sommes très attentifs. Historiquement, l'Observatoire a toujours été attentif à la façon dont sont utilisés, notamment, la cryptographie ou la capacité de reconnaissance mutuelle des acteurs. Nous l'avons fait avec les API DSP2 et les identifiants qualifiés, au sens de eIDAS version 1. Nous avons travaillé sur le quantique, qui est un des sujets sur lesquels il y a des risques pour l'intégrité et la protection des données. Nous allons continuer de suivre tout cela. Aujourd'hui, il n'y a pas encore de « *stream* » bien identifié sur ces sujets au niveau de l'OSMP, mais nous sommes disposés à échanger avec les acteurs. Nous ne demandons qu'à être convaincus.

[1] Rapport de l'Observatoire de la sécurité des moyens de paiement 2021 | Banque de France (Cf. chapitre 3 : « L'identité numérique et la sécurité des paiements »)

## Hervé Sitruk

*Sur l'identité numérique, je suggère que nous ayons une petite réunion à quelques-uns pour en parler, car que je pense que cela vaut la peine que ce sujet soit réexaminé au niveau de l'Observatoire*

*Par ailleurs, je signale que Marie-Christine Caffet (membre de l'OSMP et ancienne médiatrice auprès de la FBF) interviendra lors de notre plénière du 16 octobre pour nous présenter la vision des médiateurs notamment sur la question que tu as évoquée des progrès dans les remboursements et des litiges. Si tu es disponible le 16 octobre matin, tu seras le bienvenu.*

## Julien Lasalle

Merci Hervé, c'est noté et j'espère pouvoir venir le 16 octobre.

## Hervé Sitruk

*Vous avez vu tout à l'heure avec Éric Ducoulombier que la question de la fraude est au cœur des négociations politiques sur la DSP car c'est devenu un réel sujet de préoccupation. Nous n'avons pas abordé la question des cryptopaiements, mais peut-être devrions nous y consacrer une réunion spécifique sous l'angle de la lutte contre la fraude ou de la prévention de la fraude, afin d'objectiver cette problématique, en France et en Europe.*

## Julien Lasalle

Sur la fraude, grâce à l'OSMP la France fait son diagnostic régulièrement. Mais on nous pose souvent la question « que se passe-t-il ailleurs en Europe ? ». Je rappelle que la DSP2 a confié aux autorités le soin de collecter des données et des statistiques sur la fraude. Mais la qualité n'est pas là. Nous (l'OSMP) avons 25 ans d'expérience, avec des missions de contrôle sur place chez les banques pour nous assurer que nos méthodologies sont bien appliquées et que nous mesurons des choses comparables d'un établissement à l'autre. Mais quand on voit les taux de fraude affichés par certains pays, on se dit que ce n'est absolument pas crédible.

Les choses s'améliorent tout de même petit à petit, et on peut espérer être bientôt en mesure de faire des comparaisons et d'expliquer en quoi, à cadre réglementaire commun, la France se distingue de ses pays voisins. Nous espérons pouvoir un jour nous confronter à ce qui se passe à l'extérieur, grâce au futur observatoire européen que nous appelons de nos vœux et auquel nous serons ravis d'apporter notre savoir-faire.

## Hervé Sitruk

Merci beaucoup, Julien.

***