France Payments Forum – Plénière du 19 septembre 2024

Synthèse de l'intervention de Julien Lasalle

Banque de France, Secrétaire de l'OSMP

FRANCE PAYMENTS FORUM

Présentation du 8e rapport annuel

par

Julien Lasalle, Secrétaire de l'OSMP

Plénière du France Payments Forum
19 septembre 2024

bservatoire de la sécurité des moyens de paiement
www.observatoire-paiements.fr

Plan de la présentation

1) Vue d'ensemble

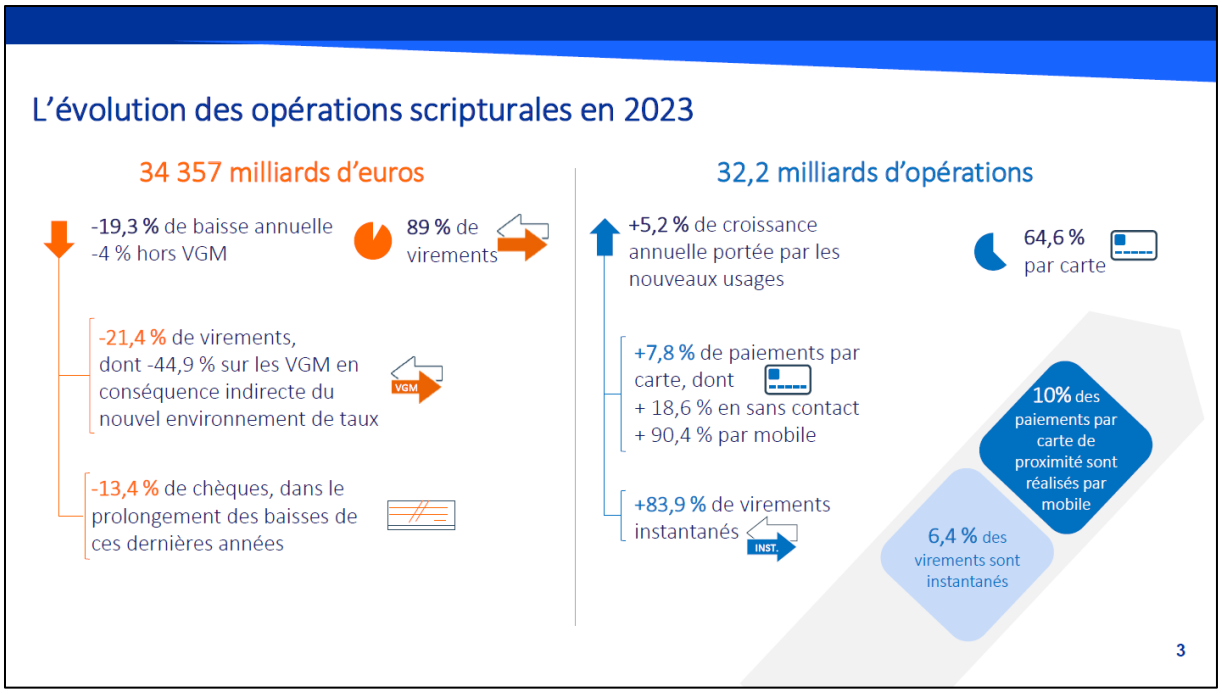
- L'évolution des transactions scripturales
- L'état de la fraude aux moyens de paiement

2) Enjeux et actions de prévention de la fraude

- Les paiements à distance
- Les paiements SEPA
- Les paiements par chèque
- L'informatique quantique

3) Priorités pour 2024-2025

2

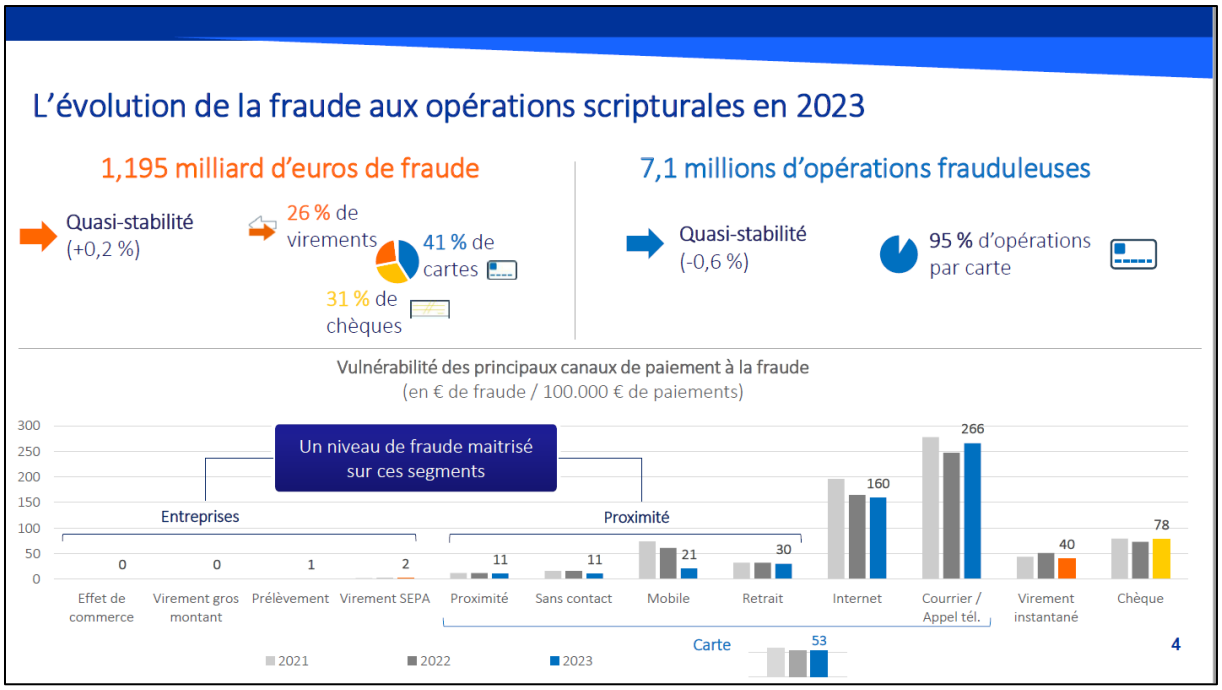


Sur l'évolution des paiements scripturaux en 2023, on note sur la partie de gauche de cette slide quelque chose qui ressemble à une bizarrerie statistique : en 2023, les flux de paiements français en valeur n'étaient « que » de 34 400 milliards d'euros, en baisse de près de 20% par rapport à l'année précédente. Si on enlève les Virements de Gros Montant (VGM), la baisse n'est plus que de 4 %, mais elle est quand même étonnante puisque du côté droit de la slide (en nombre d'opérations), les paiements scripturaux continuent à se développer (+ 5,2%).

Cette bizarrerie statistique est liée à la remontée des taux directeurs de la Banque Centrale Européenne. On a en effet découvert à cette occasion qu'en période de taux négatifs, certaines grandes administrations publiques avaient développé des pratiques de trésorerie consistant à faire des virements de compte à compte d'un établissement à l'autre pour aller « chercher du rendement » et à rapatrier éventuellement les fonds ensuite, générant ainsi des montants de flux très importants pour des nombres d'opérations très limités. C'est ce qui explique, pour l'essentiel, cette baisse des montants échangés par virement.

Le seul instrument de paiement dont la baisse se poursuit, en montant comme en nombre d'opérations, est le chèque, puisqu'on est au-dessus des 10% de baisse annuelle.

La croissance du nombre d'opérations est surtout liée aux nouveaux usages : paiement sans-contact, paiement mobile et virement instantané. En 2023, 10% des paiements par carte en magasin étaient faits par mobile et 6% des virements étaient des virements instantanés. Ces ordres de grandeur ont dû largement évoluer en 2024 car cette dynamique se poursuit.



J'en viens maintenant aux **statistiques de fraude**. On note une grande stabilité, en valeur comme en nombre d'opérations frauduleuses.

Le **chèque** reste un instrument de paiement sur-fraudé : si on regarde le coût par instrument de paiement, le chèque a le taux de fraude le plus élevé à 78 euros de fraude pour 100 000 euros de paiement, devant la carte qui est à 53 euros. Sur les paiements SEPA, les paiements du segment entreprises sont importants, donc le dénominateur est très élevé et par conséquent le taux de fraude est très faible.

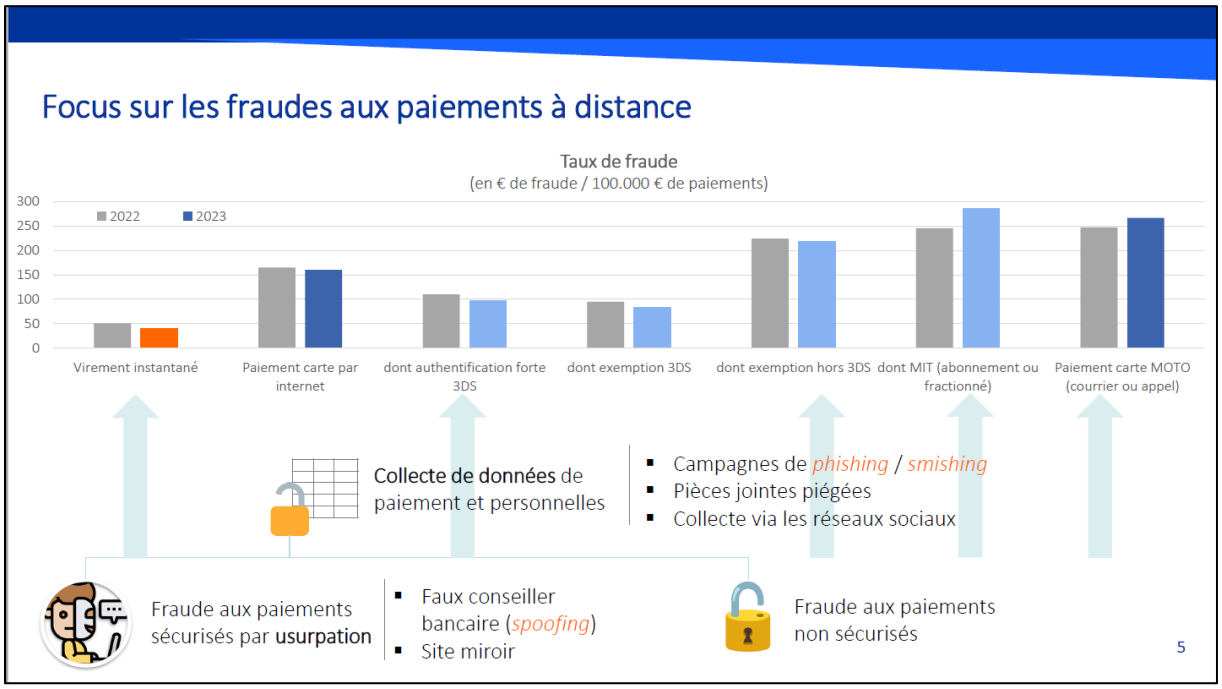
Sur le segment des paiements de proximité, la partie carte (où on s'appuie sur la remarquable technologie des cartes à puce qui continue de protéger les porteurs français), des dispositifs comme les plafonds en sans contact permettent d'avoir un niveau de fraude à son plus bas niveau historique.

Également sur les paiements de proximité, un point très satisfaisant est que le mobile est rentré dans le rang. On avait des fraudes à l'enrôlement, mais la mise en place de l'authentification forte sur l'enrôlement des cartes dans les mobiles a permis de revenir à un taux de fraude qui est globalement celui qu'on avait sur le sans contact il y a 3 ou 4 ans.

Notre priorité reste donc la **fraude sur les paiements à distance**, avec deux grandes familles :

- La fraude aux paiements à distance sans authentification forte. C'est la méthode classique : on collecte des données via du phishing ou des malwares, et on les réutilise ensuite sur des sites non sécurisés, pour des transactions à faible niveau de risque.

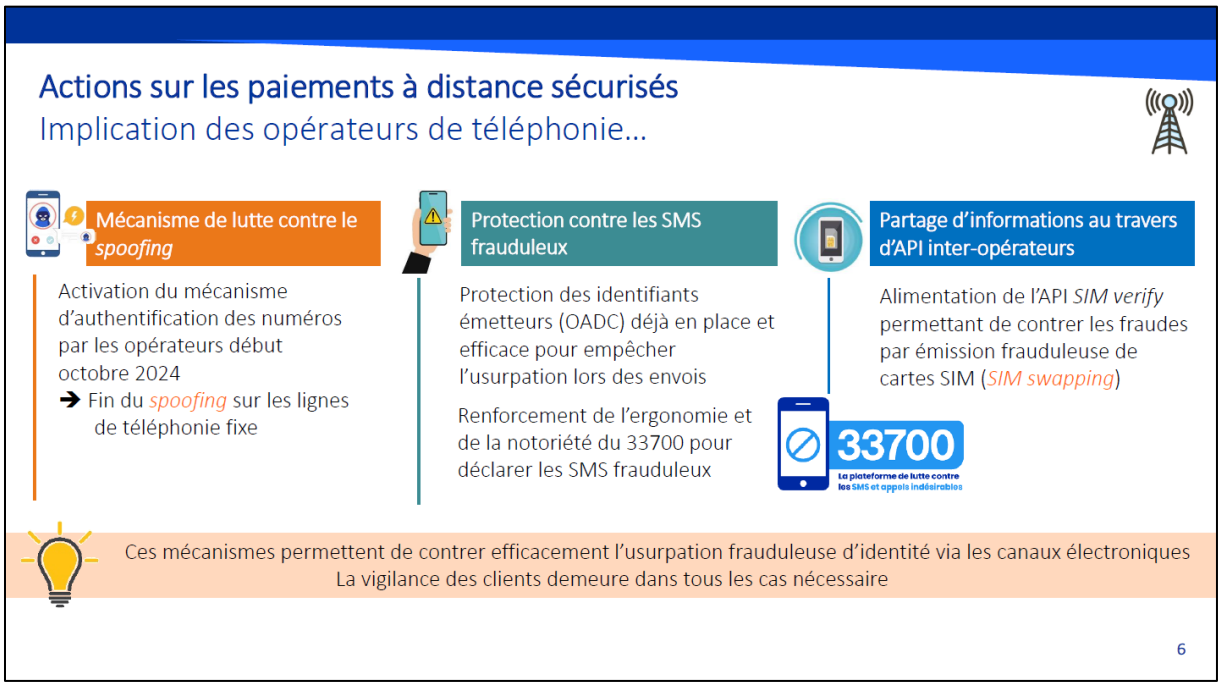
- La fraude aux paiements sécurisés avec authentification forte, avec des techniques d'usurpation et de manipulation dans lesquelles le fraudeur va :
  - Soit essayer de prendre la main sur les outils d'authentification, donc manipuler un interlocuteur de la chaîne des paiements qui peut être la banque elle-même, l'opérateur de téléphonie ou le porteur, pour opérer un transfert du moyen d'authentification,
  - Soit s'attaquer au porteur lui-même : c'est la fameuse fraude au « faux conseiller » bancaire.



Pour donner un ordre de grandeur, on estime la fraude par manipulation, donc la fraude au paiement internet sécurisé par carte et virement sur les banques en ligne à un peu moins de 340 millions d'euros en 2023, ce qui représente un tiers de la fraude aux moyens de paiement, contre 20% deux ans plus tôt. Un phénomène qui se développe est celui des fraudes par usurpation.

Il n'en demeure pas moins que les canaux de sécurisation des paiements en ligne, notamment 3-D Secure, présentent des taux de fraude qui sont les plus bas parmi les paiements à distance et qui continuent à s'améliorer, puisqu'on est passé sous la barre des 1 pour 1 000, à la différence de ce qui se passe en dehors de 3-D Secure, avec les pratiques de type *Direct to Authorization* promues par Visa notamment, sur lesquelles on ne sait visiblement pas aussi bien gérer le risque des exemptions puisque les taux de fraude sur les exemptions y sont deux fois et demi plus élevés. J'y reviendrais plus loin, mais ça nous questionne sur notre neutralité technologique : quand on a un tel écart entre deux canaux, il vient un moment où on ressent la responsabilité de devoir en imposer un plutôt que l'autre.

Et puis, il y a les vulnérabilités qu'on connaît bien depuis quelques années sur les paiements MIT et MOTO. Ce qui est inquiétant sur ces canaux, c'est que non seulement qu'ils sont 2,5 à 3 fois plus vulnérables que 3D Secure, mais en outre, que le taux de fraude continue à progresser alors que les usages progressent. Les MIT et MOTO ne sont pas un segment encore très utilisé, mais le fait que le taux de fraude soit structurellement très élevé nous inquiète.



La nouveauté de 2023-2024 a été l'arrivée des opérateurs de téléphonie et de leur régulateur, l'ARCEP, au sein de l'Observatoire. Cela nous a amenés à diversifier nos actions sur **trois grands sujets.**

- **La lutte contre le spoofing**. En vertu de la loi Naegelen les opérateurs étaient censés authentifier les numéros d'appel depuis juin 2023. Mais cela nécessitait une mise à jour d'infrastructures qui est à peu près l'équivalent de ce que nous avons dû faire avec 3-D Secure dans le monde des paiements, et les opérateurs ont eu un an de retard. On peut certes leur jeter la pierre, mais il faut quand même se rendre compte des efforts que nécessite une migration de cette ampleur.

  Donc à partir de début octobre 2024, les opérateurs vont couper les appels qui ne comportent pas le certificat d'authenticité du numéro d'appelant, c'est-à-dire que si quelqu'un a trafiqué le numéro et qu'il n'est cohérent avec le certificat (si le certificat est corrompu, inconnu ou manquant), les opérateurs auront la responsabilité de couper les appels sans les faire parvenir à leur destinataire.

  Nous avons de grandes attentes à l'égard de ce mécanisme, mais soyons clairs : pour une bonne partie de la fraude au conseiller bancaire, on nous rapporte qu'il n'y avait pas de

spoofing, mais juste un « conseiller bancaire » très convaincant et capable de dire à sa victime : « j'ai vu que vous avez donné ce matin même vos données sur un site de phishing en pensant payer une amende ou changer votre carte vitale » Et cela suffit à convaincre la victime qu'elle est contactée par un vrai service anti-fraude. Donc, il ne faut pas s'imaginer que la lutte anti-spoofing fera disparaître du jour au lendemain les fraudes par manipulation. Il y a aussi une question de vigilance de l'utilisateur et de bon comportement. J'y reviendrai.

- **La protection contre les SMS frauduleux**. Là aussi, d'excellentes choses ont été faites par les opérateurs depuis un certain temps. Vous avez dû noter comme moi qu'on ne reçoit plus de SMS frauduleux qui usurpent le nom d'expéditeur. Il n'y a plus de faux SMS dont l'émetteur affiché est une caisse d'épargne, Ameli ou les impôts. Mais les fraudeurs sont malins : maintenant, ils envoient des SMS depuis des 06 ou des 07 et ils mettent en majuscules, sur la première ligne, AMELI, GLS Logistique ou autres noms connus, et finalement, le consommateur ne fait pas très attention et il continue de cliquer ou d'appeler le numéro sur le SMS. Là aussi, c'est la vigilance des utilisateurs qu'il faut continuer à stimuler.

  Il faut aussi saluer les efforts qui ont été faits par rapport au 33 700 et rappeler qu'un utilisateur qui déclare un SMS frauduleux au 33 700 ne se protège pas lui-même (puisqu'il a déjà identifié que le SMS est frauduleux) mais protège les autres. Il y a des mécanismes inter-opérateurs qui font que quand un expéditeur commence à envoyer beaucoup de SMS frauduleux et qu'il est notifié au 33 700, normalement, les opérateurs coupent l'acheminement de ces SMS.

- **Le partage d'informations au travers d'API inter-opérateurs,** avec par exemple l'API SIM Verify qui est aujourd'hui disponible et couvre désormais tous les grands opérateurs. Les banques qui font de l'authentification par SMS OTP renforcé peuvent utiliser cette API pour voir s'il n'y a pas eu de réémission de carte SIM au cours d'une certaine période.

  Cette application est payante, et il y a donc logiquement une question de business model. Certains établissements qui ont testé l'application nous ont dit que ce qu'ils gagnent contre la fraude est suffisamment rentable pour justifier le recours à l'application... Je laisse à chacun le soin de faire ses expériences. Il est évident qu'on ne peut pas demander à des opérateurs de télécoms de mettre à jour gratuitement des données via ce système d'API.

  C'est une solution qui a le mérite d'exister, il reste à voir si elle vaut le coup d'être utilisée ou pas, d'être industrialisée, de n'être utilisée que dans certains cas. Je pense en effet que ça n'a aucun intérêt de faire un appel à SIM Verify pour n'importe quelle transaction. C'est plutôt pour une transaction déjà identifiée par la banque comme transaction à risque qui

mérite peut-être cet appel complémentaire. Si la carte SIM est bien restée entre les mains du porteur, ça abaisse le niveau de risque ; s'il semble que la carte SIM a été réémise, ça aggrave le niveau de risque.

Ce type d'API est intéressant. Nous sommes en train de regarder les **API** de type ScamSignal qui existent au Royaume-Uni et qui permettent de savoir si une ligne téléphonique est en cours d'utilisation. Par exemple, une banque pourrait savoir si son client est au téléphone au moment où il valide un paiement. Il y a sans doute d'autres façons de le faire, par les OS et les droits attribués aux applications bancaires.

Une des difficultés sur lesquelles on bute sur ce type d'API, c'est de savoir jusqu'à quel point on est capable de fournir des données à valeur ajoutée dans ces API. Nos confrères britanniques nous disent en effet que ça génère beaucoup de faux positifs, car il y a beaucoup de gens qui achètent tout en étant au téléphone avec leur famille ou avec des amis, par exemple pour réserver un voyage en se mettant d'accord sur la date ou sur les excursions. Donc, pour bien faire il faudrait savoir non seulement si le client est en ligne mais aussi savoir si c'est lui qui a passé l'appel ou qui a reçu l'appel (s'il a reçu l'appel, il y a plus de risques que ce soit un appel par manipulation), savoir si la conversation téléphonique a duré plus qu'un certain temps, car l'expérience montre que les fraudes par manipulation, ce sont des appels téléphoniques plus longs que la moyenne. De même, sur SIM Verify, il faudrait savoir si la carte SIM a été réémise dans la ville où réside le titulaire du compte ou ailleurs, à quel lieu précisément, à quel jour, quelle heure.

Ce sont des données à valeur ajoutée qui pourraient être remises dans ce type d'API. Ça coûterait sans doute plus cher et ça finirait par poser des vrais problèmes de conformité au RGPD. Donc, c'est une piste que nous explorons patiemment avec les opérateurs de téléphonie. Mais à ce stade, il n'y a pas de promesse que ce troisième volet sera considérablement renforcé ces prochaines années, et il y a en tout cas un vrai sujet de *business model*, sur SIM Verify, mais aussi sur ScamSignal.

Les opérateurs téléphoniques peuvent faire beaucoup de choses. On peut même se poser la question de leur responsabilité financière sur certains cas de fraude dans le cadre des futures réglementations européennes. Mais, là encore, rien de tout cela ne peut se substituer à la vigilance des utilisateurs. Et donc, il y a une question de bons réflexes.

En tout cas, les deux volets de gauche (lutte contre le spoofing et contre les SMS frauduleux) ont l'avantage de rendre les attaques plus facilement détectables. Tant qu'un fraudeur pouvait usurper un identifiant alphanumérique d'émetteur de SMS ou un numéro de téléphone bancaire, cela facilitait sa capacité à se faire reconnaître pour ce qu'il n'était pas.

Sur les paiements à distance non sécurisés (MIT, MOTO…), un plan d'action a été adopté par l'Observatoire au début de l'été visant à réserver strictement l'usage de ces canaux pour les cas les plus légitimes et à mettre un ensemble de barrières et d'exigences sur leur utilisation.

Sur les MIT, il y a la question de l'engagement initial du consommateur à payer. Il faut s'assurer qu'il y a eu une authentification forte, même si les MIT qui sont générés derrière sont tout petits et seraient éligibles aux exemptions. Dès lors qu'il y a MIT, il doit y avoir mandat et authentification forte. C'est comme pour un mandat de prélèvement : même si c'est pour payer 2 centimes, le mandat doit être signé. De même, le MIT doit être authentifié fortement et il doit prévoir les conditions dans lesquelles l'utilisateur s'engage à payer.

Ensuite, tous les flux de MIT doivent contenir la référence de ce mandat. Nous avons demandé aux banques de faire du *screening* pour identifier les commerçants qui avaient des défauts flagrants de qualité des mandats parce que la référence du mandat est invalide ou ne correspond pas à la transaction qui a été émise. L'idée, ce n'est pas de stopper ces flux en temps réel sur la base de cette analyse, mais c'est d'aller ensuite vers les commerçants concernés pour les amener à améliorer leurs pratiques.

Sur les MOTO, l'idée est aussi de réduire la capacité des utilisateurs et des commerçants à utiliser ces canaux-là, sauf dans les cas d'entreprises ou de secteurs pour lesquels ces canaux font partie de leur activité. Mais concrètement, on ne veut plus voir de cas de CIT transformés en MIT parce que la banque ou l'utilisateur n'est pas capable d'utiliser l'authentification correctement, et on ne veut pas voir de CIT transformés en MOTO.

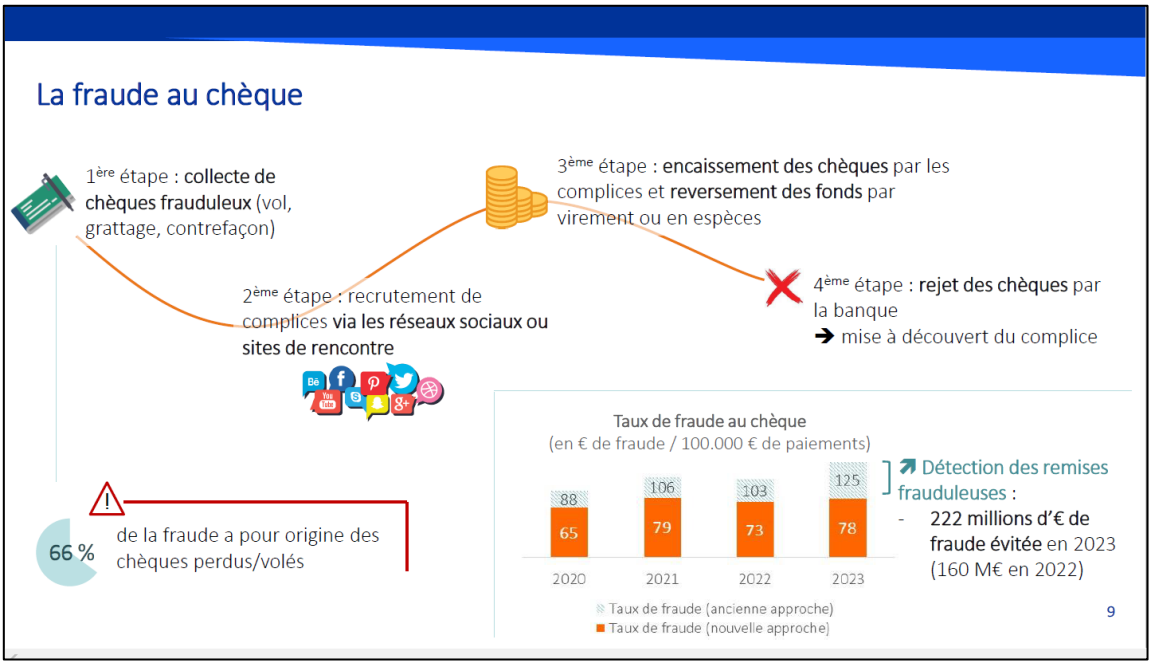
Sur les DTA (transactions exemptées hors 3-D Secure), notre but est clairement de les faire disparaître, en tout cas au-dessus d'un certain seuil. Le seuil était à 500 euros, nous l'avons abaissé à 250 euros, nous l'abaisserons à 100 euros, et peut-être encore plus bas si le taux de fraude sur ces transactions reste anormalement élevé.

Concernant les **fraudes aux paiements SEPA**, nous avons réalisé une étude sur les techniques de fraude. Sur les paiements SEPA, à la différence des paiements par carte, il y a une part importante de paiements *corporate,* avec la fraude au changement de coordonnées de paiement ou la fraude au président. Nous avons des cas de prélèvements sans mandat, quelques cas (qui font les gros titres des médias en ce moment) d'opérateurs peu scrupuleux qui n'hésitent pas à déménager leurs comptes dans d'autres pays pour continuer à faire des prélèvements frauduleux. Sur tout cela, il faut développer des réflexes de vigilance. Il y a aussi les listes blanches et listes noires qui existent par exemple sur les prélèvements.

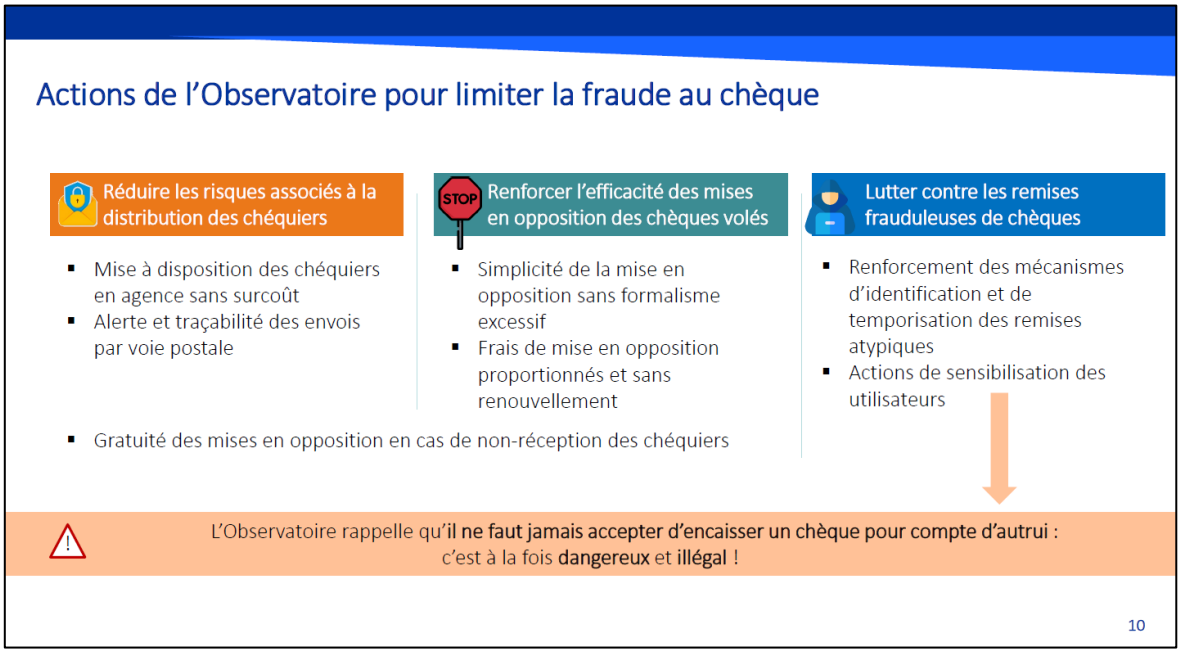
Nous fondons beaucoup d'espoirs dans les **mécanismes d'échange d'informations** entre acteurs.

- **La vérification du bénéficiaire (VoP),** qui entrera en vigueur fin 2025. Certes, la VoP n'arrêtera pas toutes les fraudes, mais elle est prévue par la loi et elle permettra tout de même d'arrêter un certain nombre de manipulations de coordonnées bancaires. Je rappelle que l'OSMP avait invité les acteurs de la place française à anticiper autant que possible l'arrivée de cette disposition.
- **Le partage d'informations** sur les cas de fraude (par exemple les IBAN ou autres attributs utilisés par les fraudeurs), dans le respect de la réglementation des données. Nous avons conduit des travaux à cet égard pour essayer de mesurer les capacités de dispositifs de ce

type, avec **deux options** : soit on attend la DSP3 et le RSP, soit on se dote d'une réglementation spécifique, en créant des exceptions au secret bancaire pour permettre aux acteurs de marché de s'échanger ces données.



Sur **la fraude au chèque**, il est important de noter que si on n'avait pas mis en place depuis quelques années des mécanismes de détection des remises fraudeuses, le taux de fraude sur le chèque ne serait pas de 78% pour 100 000, mais de 125%. Ces mécanismes ont permis d'éviter 222 millions de fraudes en 2023.



La partie droite de cette slide (**lutte contre les remises frauduleuses de chèques**) est le message que nous passons au grand public pour ne pas se retrouver à jouer le rôle de mule. Encaisser un chèque pour compte d'autrui, c'est à la fois illégal et très dangereux. Nous

répétons ce message tous les ans, mais il y a encore des gens qui continuent à jouer à ce jeu dangereux, à leurs risques et périls.

Les deux autres points très importants, et sur lesquels nous avons besoin de l'implication de la profession bancaire, sont la distribution des chéquiers et la mise en opposition des chèques volés.

Pour réduire les risques liés à la **distribution des chéquiers**, nous appelons les banques qui disposent encore d'un réseau d'agences à permettre la remise du chéquier en agence. C'est contraignant pour le client, raison de plus pour que cette remise en agence soit sans surcoût (sinon c'est la « double peine »).

L'autre point important est la **mise en opposition des chéquiers volés**. On sait que les mises en opposition de chèques servent à beaucoup de choses, y compris à générer du litige commercial puisqu'on peut faire opposition *a posteriori* (après avoir signé le chèque) alors qu'avec la carte, on est capable d'horodater la mise en opposition et les opérations de paiement. Il n'empêche que ça ne doit pas être beaucoup plus compliqué de mettre en opposition un chèque qu'une carte.

Pour la carte, l'opposition se fait par téléphone. Pour le chèque, on peut comprendre qu'une trace écrite soit nécessaire, mais pas par courrier recommandé avec accusé de réception et un ensemble de justificatifs. Il faut qu'on puisse mettre en opposition un chèque simplement et que les frais soient proportionnés. Nous ne disons pas que la mise en opposition doit être gratuite, mais quand la mise en opposition d'un chèque est facturée 30 euros, le client y renonce, donc le FNCI n'est pas alimenté et les systèmes commerçants ne permettent pas de lutter contre la fraude. Nous avons en outre découvert que certaines banques facturaient le renouvellement des mises en opposition ce qui est absurde parce que la déclaration au FNCI se fait en une fois.

Dernier point dans les actions de l'observatoire, nous faisons de la veille, en l'occurrence de la veille à long terme puisque nous avons travaillé sur **l'informatique quantique**, sujet sur lequel l'Observatoire a organisé une belle conférence en juin dernier. Je ne vais pas vous refaire ici toute l'histoire, mais l'informatique quantique c'est le risque qu'on casse les systèmes qu'on casse les systèmes de chiffrement qui sont associés aux paiements que ce soient les systèmes qui protègent les réseaux ou les systèmes qui protègent le paiement lui-même (les cartes, les interactions avec les terminaux…), avec le risque que des données soient volées ou détournées qu'on fabrique des « Yes Cards » (qui disent « oui » à chaque paiement) et que ça génère une perte de confiance pouvant déboucher sur des psychoses sur les instruments de paiement.

Et demain… l'informatique quantique :
Quels risques pour le paiement par carte ?

Le vol de données privées, voire confidentielles

- Déchiffrement des données personnelles : noms des clients, date, localisation et montant de leurs transactions
- Vulnérabilité du code PIN de la carte

La génération de paiements frauduleux par la fabrication de *Yes Card*

- Uniquement sur les paiements de proximité hors ligne, dont la sécurité ne repose que sur des algorithmes asymétriques (30% des transactions par carte aujourd'hui)
- Risque maitrisable pour tous les paiements en ligne via la mise à jour des algorithmes de chiffrement symétriques

La perte de confiance dans les infrastructures de paiement

- Vulnérabilité accrue des dispositifs centraux de chiffrement assurant la sécurité des cartes de paiement, avec des risques de devoir retirer / réémettre massivement les cartes en cas de compromission

11

Et demain… l'informatique quantique
Les recommandations de l'Observatoire pour préparer l'avenir

Objectif: préserver le haut niveau de sécurité des paiements et la confiance des utilisateurs, en anticipant les temps nécessaires d'adaptation

Au niveau de chaque établissement

1) **Inventorier** les différents dispositifs de sécurité des systèmes d'information
2) **Hiérarchiser les données** selon leur degré de sensibilité
3) **Expérimenter** l'implémentation d'algorithmes asymétriques basé sur des systèmes *hybrides* et *crypto-agiles*
4) **Constituer une feuille de route** validée à haut niveau en matière de résistance au quantique

Au niveau sectoriel et collectif

5) **Sensibiliser les autorités de standardisation** des protocoles de paiement afin d'anticiper les choix en matière de résistance au quantique

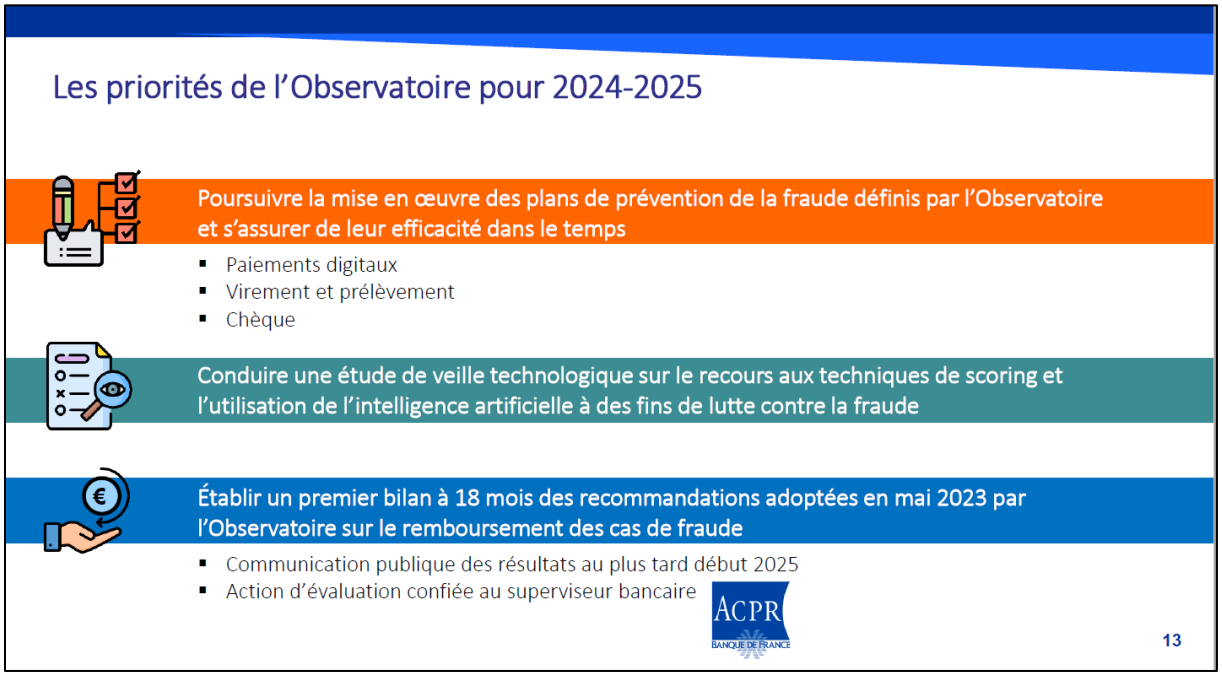
6) **Œuvrer à la création d'un groupe de travail pérenne de haut niveau**, idéalement à l'échelle européenne, regroupant notamment les grandes institutions de paiement, les autorités publiques de supervision et de standardisation

12

Les deux grands messages passés par l'Observatoire portent sur la préparation individuelle et la préparation collective.

- **Préparation individuelle** : quand on est banquier, prestataire technique, système de paiement ou réseau de paiement par carte, on doit se poser la question « Où sont mes algorithmes de chiffrement ? sont-ils résilients ? faut-il allonger les clés ? faut-il expérimenter des algorithmes un peu plus exotiques que ceux qu'on connaît depuis des décennies ? »

- **Préparation collective** : le secteur des paiements doit s'organiser, par exemple via ses autorités de standardisation, pour injecter des algorithmes résistants au quantique là où il y en a besoin, pour préparer l'avenir. Nous avons sans doute une dizaine d'années devant nous, mais il faut se préparer et le faire de manière concertée, éventuellement avec d'autres secteurs d'activité.

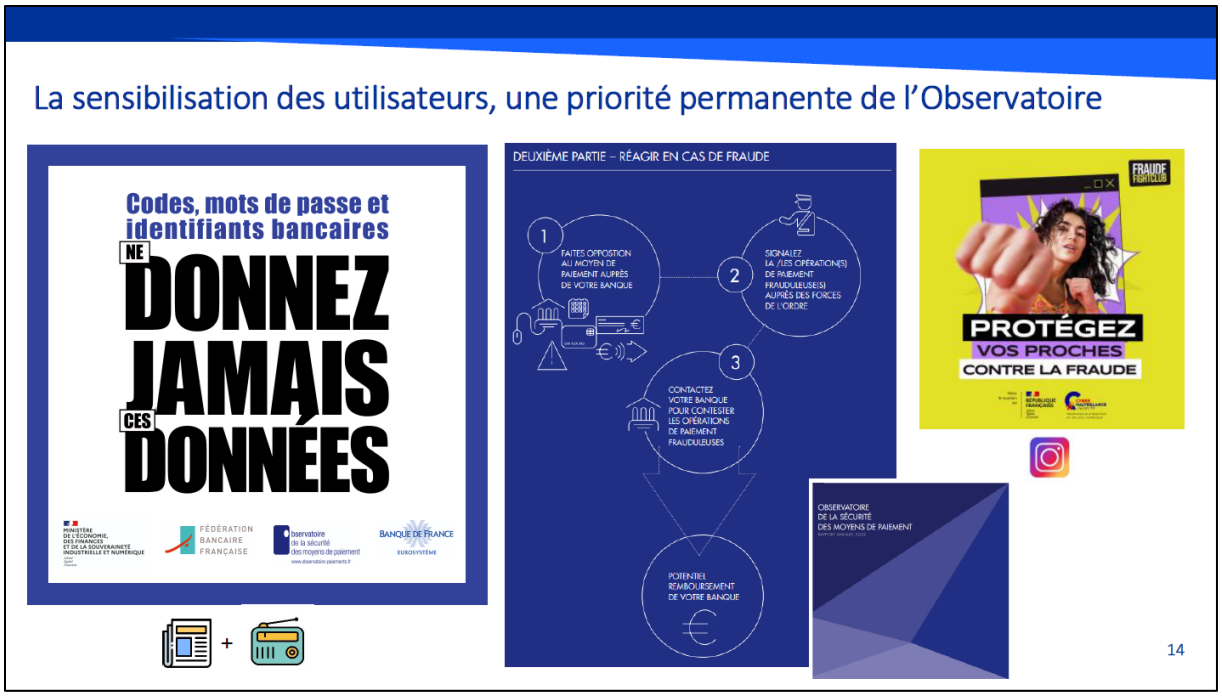


Pour conclure, **les priorités de l'OSMP pour 2024-2025** sont d'abord de poursuivre tout ce qui est fait en matière de prévention de la fraude. Notre prochaine étude de veille technologique portera sur le scoring et l'utilisation de l'intelligence artificielle à des fins de lutte contre la fraude (sujet passionnant), et nous nous intéresserons sans doute ensuite aux stablecoins et aux cryptos.

Point très important (et qui risque d'être sensible médiatiquement), nous présenterons en fin d'année le **bilan des 18 mois des recommandations de l'OSMP sur le remboursement des cas de fraude**. Des enquêtes sont en cours par l'ACPR. Le bilan sera présenté d'abord au Collège de l'ACPR puis à l'OSMP et sera rendu public, selon un processus qui s'échelonnera entre fin 2024 et début 2025.

Dernier message sur **l'appel à la vigilance**. La campagne de communication lancée conjointement par la profession bancaire et les pouvoirs publics en juin dernier a eu beaucoup d'impact. Elle va être réactivée en octobre et jusqu'à la fin de l'année. J'invite tous ceux d'entre vous qui ont des relations avec les consommateurs à relayer ces messages car on ne peut pas protéger les utilisateurs contre leur gré.

Merci de votre attention.



Questions-réponses

Question 1

a) *C'est bien d'avoir associé les opérateurs de télécommunication aux travaux de l'OSMP, mais il y a aussi beaucoup de communication qui passent par les réseaux de type WhatsApp et sont invisibles des opérateurs. Pourrait-on associer ces plateformes au groupe de travail ?*

b) *On voit arriver une nouvelle technologie appelée « rich call data », qui peut faire très mal sur les usurpations d'identité. Quelle est votre vision sur ce sujet ?*

Julien Lasalle

Je pense que nous allons progresser pas à pas dans le secteur des communications et d'internet. Nous avons commencé à regarder ce qui se passe sur le RCS (messages commerciaux notamment) puisqu'on a vu que la technologie arrive sur les nouvelles versions d'iOS. Concernant les messageries, de type WhatsApp, qui peuvent être des supports d'un certain nombre de fraudes, la question est de savoir comment discuter sur une base nationale avec des plateformes d'envergure internationale. C'est un beau challenge, mais oui, nous allons nous y attaquer. De même pour les futures technologies qui peuvent être des véhicules de fraude : nous devons être dans l'anticipation.

Question 2

Concernant le bilan des recommandations de l'OSMP sur le remboursement des cas de fraude, que se passerait-il pour les banques qui, selon l'enquête effectuée par l'ACPR, ne seraient pas en phase avec les recommandations?

Julien Lasalle

Il s'agit d'une enquête menée par l'ACPR, donc libre à elle de prendre les mesures qu'elle pourrait estimer nécessaires. Du point de vue de l'OSMP, la question est surtout de savoir si ces recommandations ont été efficaces. Si oui, il s'agira simplement d'aligner les "mauvais élèves" sur les "bons élèves", ce que l'ACPR saura faire. Si non, la question se posera d'aller vers des recommandations plus prescriptives.

J'ajoute que c'est sur ces recommandations de l'OSMP qu'a été construite la position de la France dans la négociation actuelle sur la DSP3 et le RSP. Si le bilan montre que ces recommandations sont applicables et ont eu des effets vertueux, nous resterons sur cette ligne. Si, à l'inverse, le bilan montre que ces recommandations ne sont pas applicables ou pas assez "musclées", nous verrons avec la DG Trésor s'il faut changer notre fusil d'épaule dans la négociation sur la DSP3 et le RSP et éventuellement se ranger dans le camp de certains États-membres qui ont une vision beaucoup plus dirigiste.

Question 3

Que pensez-vous du 50/50 au Royaume-Uni ?

Julien Lasalle

Je salue la créativité de nos amis britanniques. Nous en avons parlé avec des représentants d'UK Finance. Dès lors qu'on donne un droit à remboursement inconditionnel en cas de fraude jusqu'à 85 000 £, on peut craindre que certains réseaux organisés parviennent à prospérer sur ces remboursements.

Concernant le 50/50, c'est-à-dire le partage entre le banquier émetteur et le banquier récepteur des fonds, c'est conceptuellement intéressant car l'établissement qui se situe du côté du fraudeur a une responsabilité dans la fraude. Mais comment ceci peut-il s'organiser en pratique ? Si on veut "injecter" cela dans la négociation sur la DSP3 et le RSP, ça devient un jeu compliqué car on veut aussi pousser pour la responsabilisation des opérateurs de télécommunication. Mais c'est tout de même une piste de plus et il faut que la Commission, le Parlement et le Conseil en tiennent compte. Et le fait que les Anglais soient partis un peu plus tôt nous permettra peut-être de bénéficier de leur retour d'expérience.

NDR : postérieurement à la présente réunion, le régulateur britannique des paiements (PSR) a publié le 7 octobre 2024 un communiqué annonçant l'entrée en vigueur des nouvelles règles de protection des victimes « *d'Authorised Pushed Payment (APP) scams* ».

Hervé Sitruk

Une dernière question : où en est l'idée d'un OSMP européen ?

Julien Lasalle

L'ERPB (*Euro Retail Payment Board*) vient de publier un rapport de son groupe de travail sur la fraude, dont une des recommandations est la création de quelque chose d'un peu analogue à l'OSMP au niveau européen. Donc l'idée fait son chemin.

Hervé Sitruk

Merci beaucoup Julien