Interview de Denis Beau, président de l'Observatoire de la Sécurité des Moyens de Paiement

Mr le Président, le rapport de l'Observatoire sur l'année 2023 vient d'être publié. Quelles sont les principales tendances que vous en retenez en matière d'usage des moyens de paiement ?

La tendance de fond à la progression de l'usage des moyens de paiement dématérialisés se poursuit à un rythme soutenu. Les données 2023 que l'Observatoire a réunies montrent une croissance de plus de 5% des paiements scripturaux (hors espèces) avec 32,2 milliards d'opérations, ce qui constitue un niveau record. Dans ce fond de paysage, la carte conforte son statut de moyen de paiement quotidien préféré des Français, avec une part dans le nombre des transactions scripturales qui s'approche désormais des deux tiers (64,6%) : le nombre de paiements par carte progresse aussi bien en proximité (+7%), c'est-à-dire principalement en magasin, que sur internet (+12%), ce dernier canal bénéficiant de la croissance du e-commerce et des usages numériques.

Quand on regarde de plus près, cette croissance des paiements scripturaux est notamment alimentée par les usages les plus innovants : le paiement mobile dont les flux doublent quasiment chaque année (+90% en 2023) représente désormais 10% des paiements par carte en proximité ; le virement instantané continue aussi de se développer rapidement (+84% en nombre de transactions), représentant désormais 6,4% des virements. À contre-courant de ces tendances, l'utilisation du chèque poursuit sa décrue et ne représente plus que 2,8 % des transactions (contre 14,4% en 2013).

...et en matière de fraude ?

Avec les membres de l'Observatoire, je me réjouis d'observer une stabilité générale de la fraude, tant en nombre de cas (de l'ordre de 7 millions) qu'en montant (1,2 milliard d'euros). Cette stabilité mérite d'être saluée, alors même que l'usage des moyens de paiement scripturaux progresse, que le niveau de menace des fraudeurs reste élevé et que leur sophistication augmente, dans un contexte géopolitique de tensions. Ces bons résultats sont le signe de l'engagement de l'ensemble des acteurs de la chaîne des paiements dans la lutte contre la fraude. Ceux-ci sont tous rassemblés au sein de l'Observatoire, des commerçants aux acteurs bancaires, des consommateurs aux autorités régaliennes, autour de la promotion de ce bien commun qu'est la sécurité de nos moyens de paiement.

Au-delà des évolutions annuelles, il y a quelques tendances structurelles qui ressortent des statistiques de fraude qu'élabore l'Observatoire. Certaines sont positives, comme la baisse de 38% du taux de fraude sur les paiements par carte sur internet entre 2018 et 2023. Cette baisse est incontestablement le fruit de la mise en œuvre des règles d'authentification forte, souhaitées par les régulateurs européens, et qui se sont déployées à partir de 2019 sous l'égide de l'Observatoire. À cet égard, nous avons été précurseurs en France puisque des actions ont été engagées pour introduire ces dispositifs particulièrement efficaces dès la fin des années 2000. Le taux de fraude sur le virement instantané reste lui aussi maîtrisé (0,040% en 2023 soit un niveau inférieur à celui de la carte), ce qui confirme l'utilité et l'efficacité de l'authentification forte mais aussi la montée en puissance des mécanismes d'évaluation des risques en temps réel déployés par les banques et les systèmes de paiement. Sur le chèque, l'Observatoire note également des signaux encourageants en termes de sécurité, même si ce moyen de paiement affiche le taux de fraude le plus élevé dans notre gamme de moyens de paiement scripturaux.

Cela étant, nous avons encore des marges significatives de progrès et nous devons répondre au développement des nouvelles techniques de fraude. C'est pourquoi, depuis juin, l'Observatoire déploie un plan de sécurisation des paiements par carte à distance, qui ne transitent pas par les protocoles sécurisés de type 3D-Secure.

Dans le domaine du chèque, qui représente encore 31% des montants de fraude pour moins de 3% des transactions, il y a également des marges de progrès, qui sont à notre portée, même si l'usage de ce moyen de paiement est en forte baisse: la mise en opposition d'un chéquier volé devrait être aussi facile que la mise en opposition d'une carte, et celle-ci doit être gratuite si le chéquier a été volé lors de son acheminement postal. J'invite également les consommateurs à récupérer, autant que possible, leur nouveau chéquier en agence.

Quelles évolutions notez-vous dans les procédés utilisés par les fraudeurs ?

Il y a encore quelques années, l'attention de l'Observatoire portait sur certains cas de fraude, touchant principalement les entreprises et les administrations, comme la « fraude au Président », qui consiste pour le fraudeur à usurper l'identité d'un haut responsable hiérarchique et à tenter de faire exécuter des opérations de paiement par un employé. Si cette typologie n'a bien sûr pas complètement disparu et que la vigilance des services comptables reste de mise, je note que les paiements émis par les professionnels (effets de commerce, prélèvement, virements initiés par les canaux télématiques) présentent des taux de fraude très faibles, grâce à de bonnes pratiques très répandues en termes de sécurité des connexions et de mécanismes de contrôle.

En revanche, à la suite de la mise en place de l'authentification forte, les fraudeurs se sont adaptés et tournés vers des techniques de manipulation de leurs victimes. On estime que ces cas de fraude représentent aujourd'hui 379 millions d'euros, soit près de 32% des montants de fraude. Au préalable, et ce n'est pas nouveau, les fraudeurs collectent des données personnelles et de paiement par hameçonnage via des SMS ou des courriels frauduleux. Ensuite, et c'est là qu'est la nouveauté, les fraudeurs usurpent l'identité d'une personne de confiance, comme un conseiller bancaire ou encore un représentant d'une administration publique, pour faire valider les opérations frauduleuses par les victimes elles-mêmes, en jouant notamment sur la peur et l'urgence de la situation.

Face à ces techniques de manipulation, il y a bien sûr des développements techniques possibles. C'est la raison pour laquelle l'Observatoire s'est attaché à renforcer sa coopération avec le secteur des télécoms, en accueillant leurs représentants en son sein et en travaillant avec eux pour soutenir la mise en place de solutions de protections des identifiants de communication des professionnels sur leurs réseaux. Certaines sont déjà déployées ou vont prochainement l'être : c'est le cas de la protection des identifiants émetteurs de SMS ou encore de la mise en œuvre, à partir d'octobre prochain, du Mécanisme d'Authentification des Numéros (MAN), qui devrait empêcher un fraudeur d'usurper le numéro de ligne fixe d'une banque pour tromper sa victime.

Mais ces mesures techniques ne pourront être pleinement efficaces que si les utilisateurs adoptent les bons réflexes. La vigilance des utilisateurs demeure une nécessité, et c'est pourquoi les actions de sensibilisation sont donc aussi une priorité de l'Observatoire. Après une première campagne en juin dernier, rappelant un principe simple (« *Codes, mots de passe et identifiants bancaires : ne donnez jamais ces données* »), une deuxième vague de communication sera lancée en octobre 2024 sur les médias et réseaux sociaux, en association avec le Ministère de l'économie et des finances et la Fédération bancaire française (FBF).

Face à ces évolutions en matière d'usage et de fraude, quelles vont être les priorités de travail de l'Observatoire en 2025?

Beaucoup de travaux ont été engagés sur l'ensemble des moyens de paiement, et en particulier les plus vulnérables. Une première priorité est de veiller à la bonne mise en œuvre des recommandations de l'Observatoire dans le temps. C'est par exemple le cas des recommandations émises en 2023 sur le remboursement des victimes de fraude, et notamment des fraudes par manipulation, qui ont précisé les conditions d'application de la réglementation en vigueur en France. Des enquêtes sont actuellement menées par l'Autorité de contrôle prudentiel et de résolution (ACPR) et l'Observatoire sera particulièrement attentif à ces résultats, nous en ferons état début 2025 au plus tard. La bonne application des règles de remboursement est une condition de confiance des utilisateurs dans leurs moyens de paiement et de bon fonctionnement des paiements dans notre économie.

Dans le cadre de sa mission de veille technologique, l'Observatoire doit aussi s'efforcer d'anticiper les nouvelles menaces. Dans son rapport 2023, l'Observatoire a publié une étude inédite sur les risques que pourrait faire peser l'informatique quantique sur la sécurité des paiements par carte. Cette étude vise à contribuer à une prise de conscience nécessaire, car la résistance au quantique doit se préparer et se planifier dans les faits dès aujourd'hui.

Pour les mois qui viennent, nos travaux de veille vont se concentrer sur les méthodes de *scoring* et l'utilisation de l'intelligence artificielle. Ces techniques sont essentielles dans un monde où l'instantanéité des paiements devient progressivement la norme et où les contrôles en amont des transactions doivent être de plus en plus efficaces et réactifs. Ces travaux seront restitués en 2025 dans notre prochain rapport annuel, alors même qu'entrera en application le nouveau règlement européen sur le virement instantané, qui devrait fortement soutenir la croissance des paiements en temps réel.