

1. [Accueil](#)
2. Entity Print

Interview

[Sous-gouverneurs](#)

Les Echos : « La lutte contre la fraude est un bien commun »

Les intervenants

Denis Beau Intervention

Denis Beau, Premier sous-gouverneur de la Banque de France

25 Mai 2023

Denis Beau Intervention

Interview de Denis Beau, Premier sous-gouverneur de la Banque de France.

Les moyens de paiement évoluent pour devenir de plus en plus dématérialisés et rapides et ainsi répondre aux attentes d’instantanéité des utilisateurs. Pour la Banque de France, ces innovations requièrent la mise en place de nouveaux dispositifs de sécurité afin de contrer les risques de fraude.

Comment la fraude évolue-t-elle ?

Le montant de la fraude est stable depuis 2019 et s’est établi à 1,2 milliards d’euros. Dans un contexte d’augmentation du volume des paiements scripturaux, les taux de fraude s’orientent donc à la baisse. Nous constatons néanmoins une recrudescence de la fraude par manipulation qui touche toutes les entreprises, des plus grandes aux plus petites. Le fraudeur se fait passer de façon crédible pour un responsable de haut niveau de l’entreprise ou un fournisseur en vue de faire émettre un virement à son profit. Le taux de fraude du virement reste néanmoins très bas car il s’appuie sur des socles technologiques modernes et sûrs.

De votre point de vue, les entreprises sont-elles suffisamment attentives à ces risques ?

La Banque de France œuvre beaucoup pour sensibiliser les utilisateurs, dont les entreprises, aux risques de fraude. Tous les ans, l’Observatoire de la Sécurité des Moyens de Paiement partage son analyse pour aider les acteurs à anticiper et comprendre les nouvelles techniques de fraude. Ce travail nourrit des préconisations technologiques et comportementales. C’est un élément très important de la confiance dans la monnaie, qui est la mission de la Banque de France. Mon sentiment est que la lutte contre la fraude est un bien commun.

Quels sont les axes d’amélioration identifiés par la Banque de France ?

Les entreprises doivent faire porter leurs efforts sur deux points :

- Le respect des procédures de validation internes, fondées sur la méthode dite des quatre yeux. Toute personne à l'initiative d'un ordre de paiement doit se faire contrôler par un tiers légitime.
- Mieux comprendre la sensibilité des bases de données bancaires qui sont utilisées pour initier des ordres de paiement. Tout changement dans cette base peut être une fenêtre d'opportunité pour des fraudes. D'où l'importance de bonnes pratiques quand on procède à des changements pour vérifier qu'on n'est pas en train de substituer aux bonnes coordonnées celles d'un fraudeur.

La dématérialisation des moyens de paiement génère-t-elle plus de fraude ?

Bien au contraire. Le papier est le support le plus vulnérable et le chèque le moyen de paiement le plus fraudé (0,072%). Pourquoi ? Parce que les méthodes d'authentification ne sont pas aussi performantes que celles des moyens de paiement électroniques. C'est pour cela que la France s'est dotée d'une stratégie visant à promouvoir les moyens de paiement dématérialisés, qui sont les plus robustes.

Quel doit être le rôle des banques commerciales vis-à-vis de la lutte contre la fraude, notamment sur les paiements instantanés qui nécessitent un contrôle en temps réel ?

La directive européenne DSP 2, qui impose le recours à l'authentification forte et la protection des données de paiement (comme les IBAN) par des techniques de chiffrement, tant dans les bases de données que dans les flux échangés, a poussé les banques à renforcer leur socle technologique. La généralisation de ces procédés à l'ensemble de la zone euro permet d'améliorer la résilience face à la fraude. Les outils de scoring, qui ont recours à l'intelligence artificielle pour identifier les paiements à risque, sont appelés à se développer pour offrir un haut niveau de sécurité technique.

Face à ces renforcements technologiques, les techniques de fraude évoluent. Comment en venir à bout ?

La technologie peut être une des réponses mais elle ne doit pas être la seule car les attaques se déplacent vers l'humain. Les fraudeurs ne s'engagent plus dans une lutte technologique avec les acteurs bancaires. Ils tentent d'identifier le maillon faible, qui est souvent l'utilisateur. Un moyen de paiement technologiquement très bien protégé, s'il n'est pas utilisé conformément aux préconisations, ouvre une fenêtre de vulnérabilité qui peut être facilement exploitable. Avoir les bons réflexes est important, d'où le travail de veille que nous menons pour sensibiliser les utilisateurs aux nouvelles techniques de fraude. La technologie ne fait pas tout mais c'est un socle important, qu'il faut entretenir.

Les dirigeants ont parfois l'impression d'être engagés dans une course technologique sans fin. Quelle attitude adopter pour ne pas se décourager ?

La digitalisation de l'économie et des processus accroît l'exposition aux risques d'attaque. La meilleure garantie que l'on peut se donner, c'est d'adapter régulièrement son dispositif technique et de mettre à jour ses bonnes pratiques. Ces efforts collectifs portent leurs fruits, avec des niveaux de fraude maîtrisés.

Quels changements anticipez-vous en matière de sécurisation des moyens de paiement ?

Nous anticipons la diffusion de nouveaux outils d'identification plus ergonomiques qui vont permettre de fluidifier le parcours clients et l'acte d'achat, comme la biométrie pour le paiement mobile. Nous pensons ainsi que les systèmes d'authentification reposant sur l'identité numérique devraient se diffuser très largement, notamment au sein des entreprises. L'utilisation des cartes à puce permet déjà d'aller très loin.

La fraude sur les cryptoactifs est de plus en plus avancée. Quelles sont les solutions à déployer pour identifier les schémas de fraude et s'en prémunir ?

La fraude sur les cryptoactifs prend principalement deux formes : celle d'arnaques à travers la promotion de cryptoactifs qui n'existent pas ou dont la valeur est artificielle, et de cyberattaques qui visent à voler les stocks de cryptoactifs. C'est la raison pour laquelle nous conseillons de ne traiter qu'avec des plateformes qui ont été enregistrées, voire agréées, par l'AMF (Autorité des marchés financiers).

Comment réguler sans entraver ?

La sécurité n'est pas antinomique de l'innovation. La réglementation doit s'adapter pour favoriser l'innovation dans un cadre de confiance, donc de sécurité, au service tant des nouveaux entrants, comme les acteurs de la tech, que d'acteurs régulés issus du monde financier dit « traditionnel ». J'observe que la phase de développement des cryptoactifs avec un encadrement minimal et inégal selon les pays a donné lieu à des défaillances graves. Pour assurer le développement de cet écosystème, qui peut apporter des améliorations en matière de moyens de paiement, il y a des conditions à remplir : des exigences minimales en matière de sécurité et de protection de l'utilisateur.