Présentation du 8e rapport annuel

par Denis Beau, Président
et Julien Lasalle, Secrétaire

Conférence de presse du 10 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

L'évolution des opérations scripturales en 2023

34 357 milliards d'euros

-19,3 % de baisse annuelle
-4 % hors VGM

89 % de virements

-21,4 % de virements, dont -44,9 % sur les VGM en conséquence indirecte du nouvel environnement de taux

VGM

-13,4 % de chèques, dans le prolongement des baisses de ces dernières années

32,2 milliards d'opérations

+5,2 % de croissance annuelle portée par les nouveaux usages

64,6 % par carte

+7,8 % de paiements par carte, dont
+ 18,6 % en sans contact
+ 90,4 % par mobile

+83,9 % de virements instantanés

INST.

10% des paiements par carte de proximité sont réalisés par mobile

6,4 % des virements sont instantanés

L’évolution de la fraude aux opérations scripturales en 2023

1,195 milliard d’euros de fraude

Quasi-stabilité
(+0,2 %)

26 % de virements

41 % de cartes

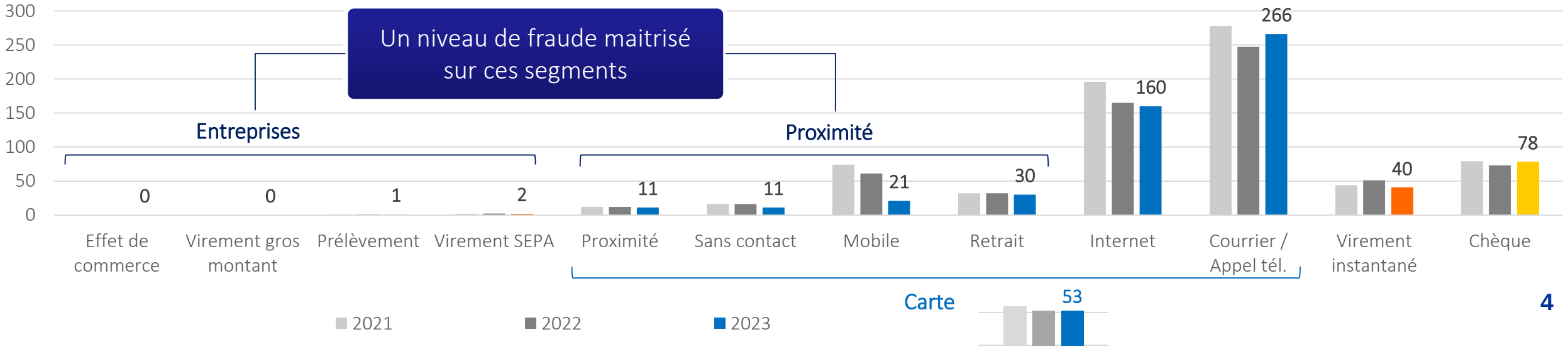
31 % de chèques

7,1 millions d’opérations frauduleuses

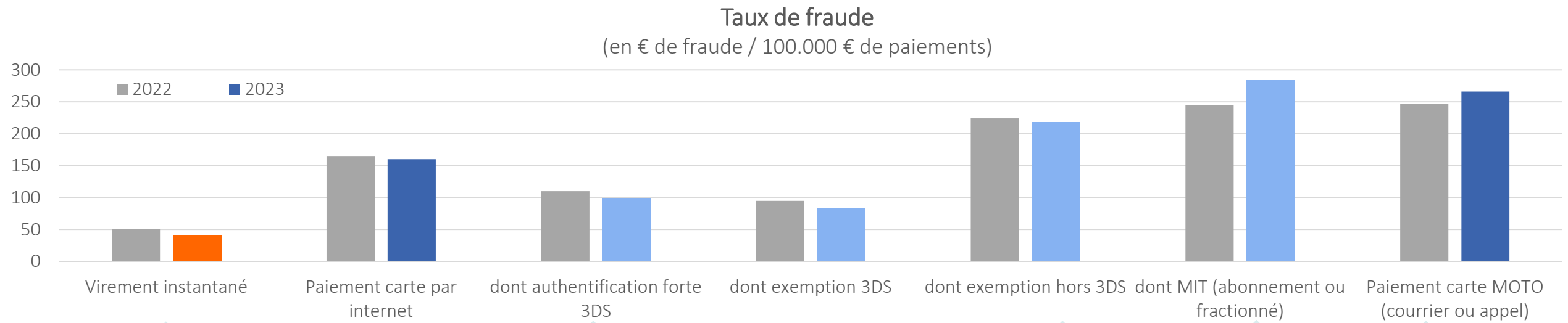
Quasi-stabilité
(-0,6 %)

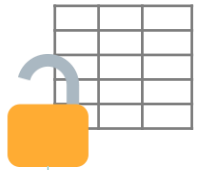
95 % d’opérations par carte

Vulnérabilité des principaux canaux de paiement à la fraude
(en € de fraude / 100.000 € de paiements)



Focus sur les fraudes aux paiements à distance





Collecte de données de paiement et personnelles

- Campagnes de *phishing* / *smishing*
- Pièces jointes piégées
- Collecte via les réseaux sociaux

Fraude aux paiements sécurisés par **usurpation**

- Faux conseiller bancaire (*spoofing*)
- Site miroir

Fraude aux paiements non sécurisés

Actions sur les paiements à distance sécurisés

Implication des opérateurs de téléphonie…

Mécanisme de lutte contre le *spoofing*

Activation du mécanisme d'authentification des numéros par les opérateurs début octobre 2024

➔ Fin du *spoofing* sur les lignes de téléphonie fixe

Protection contre les SMS frauduleux

Protection des identifiants émetteurs (OADC) déjà en place et efficace pour empêcher l'usurpation lors des envois

Renforcement de l'ergonomie et de la notoriété du 33700 pour déclarer les SMS frauduleux

Partage d'informations au travers d'API inter-opérateurs

Alimentation de l'API *SIM verify* permettant de contrer les fraudes par émission frauduleuse de cartes SIM (*SIM swapping*)

Ces mécanismes permettent de contrer efficacement l'usurpation frauduleuse d'identité via les canaux électroniques
La vigilance des clients demeure dans tous les cas nécessaire

Actions sur les paiements à distance sécurisés

Implication des opérateurs de téléphonie… et vigilance des utilisateurs

Mécanisme de lutte contre le *spoofing*

Protection contre les SMS frauduleux

Partage d'informations au travers d'API inter-opérateurs

Trois **règles d'or** à retenir pour savoir réagir face aux tentatives d'usurpation

Un banquier qui vous appelle n'a jamais besoin que vous lui communiquiez des identifiants ou que vous réalisiez des opérations

« Standard anti-fraude de votre Banque, j'ai besoin de votre identifiant bancaire et de vous faire valider des opérations via votre application mobile pour protéger vos comptes… »

Un service public, un établissement financier ou une grande entreprise n'envoie jamais de SMS depuis une ligne mobile (06 ou 07)

07 12 34 56 78

AMELIE
Renouvellement de votre carte vitale
…

Allez sur les sites internet par vos propres moyens : n'utilisez jamais les liens contenus dans des mails, sms, publicités

06 87 65 43 21

Compte client MyTravel
Offres flash à partir de 8 € / jour all inclusive
www.mytrwel.sg

Actions sur les paiements à distance non sécurisés

Traitement des paiements à distance les plus vulnérables

Sécurité : - → +

MO
Mail Order

Paiement au moyen d'un formulaire papier rempli par le payeur

TO
Telephone Order

Paiement lors d'une conversation téléphonique en fournissant le numéro de carte à son interlocuteur

MIT
Merchant Initiated Transaction

Paiement résultant d'une souscription d'abonnement ou d'une offre de paiement fractionné

CIT–DTA
Customer Initiated Transaction – Direct to Authorisation

Paiement pour lequel le commerçant sollicite une exemption d'authentification forte en-dehors de 3-DS

L'Observatoire a adopté un plan d'actions visant à **restreindre ces usages aux seuls cas légitimes, sûrs et sans alternative**, en limitant les possibilités de contournement et en favorisant le recours à des modes mieux sécurisés

Les fraudes aux paiements SEPA

Des techniques de fraude basées sur l'ingénierie sociale et l'usurpation d'identité

- Fraude au Président
- Fraude au changement de coordonnées de paiement
- Fraude au faux conseiller bancaire
- Prélèvement sans mandat

L'Observatoire a identifié des leviers complémentaires pour contrer ces types de fraude

Vigilance et bonnes pratiques des utilisateurs :

- En entreprise, par le respect des procédures internes : validation 4 yeux, contre-appel au fournisseur
- Sur le prélèvement : réactivité aux alertes et débits annoncés, listes blanches/noires

Mise en place de **dispositifs de partage de données** pour mieux identifier les paiements à risque

- Système de vérification du bénéficiaire de virement attendu d'ici octobre 2025
- Partage de données de fraude prévu par le projet de réglementation européenne DSP3/RSP

La fraude au chèque

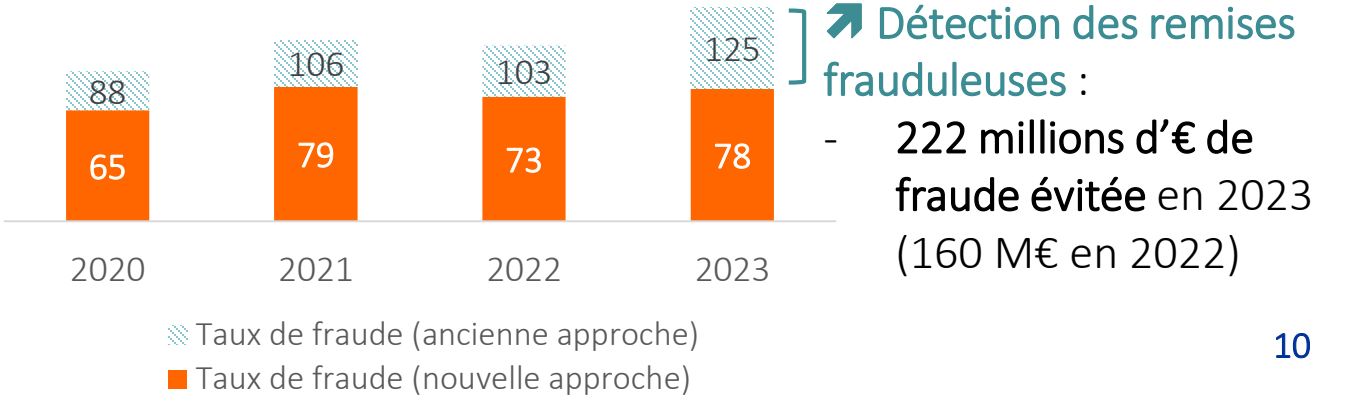
1ère étape : **collecte de chèques frauduleux** (vol, grattage, contrefaçon)

2ème étape : recrutement de complices **via les réseaux sociaux ou sites de rencontre**

3ème étape : **encaissement des chèques** par les complices et **reversement des fonds** par virement ou en espèces

4ème étape : **rejet des chèques** par la banque
➔ mise à découvert du complice

66 % de la fraude a pour origine des chèques perdus/volés



Détection des remises frauduleuses :

- **222 millions d'€ de fraude évitée** en 2023 (160 M€ en 2022)

Actions de l'Observatoire pour limiter la fraude au chèque

Réduire les risques associés à la distribution des chéquiers

- Mise à disposition des chéquiers en agence sans surcoût
- Alerte et traçabilité des envois par voie postale

Renforcer l'efficacité des mises en opposition des chèques volés

- Simplicité de la mise en opposition sans formalisme excessif
- Frais de mise en opposition proportionnés et sans renouvellement

Lutter contre les remises frauduleuses de chèques

- Renforcement des mécanismes d'identification et de temporisation des remises atypiques
- Actions de sensibilisation des utilisateurs

- Gratuité des mises en opposition en cas de non-réception des chéquiers

L'Observatoire rappelle qu'**il ne faut jamais accepter d'encaisser un chèque pour compte d'autrui** :
c'est à la fois **dangereux** et **illégal** !

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

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

Les priorités de l'Observatoire pour 2024-2025

Poursuivre la mise en œuvre des plans de prévention de la fraude définis par l'Observatoire et s'assurer de leur efficacité dans le temps

- Paiements digitaux
- Virement et prélèvement
- Chèque

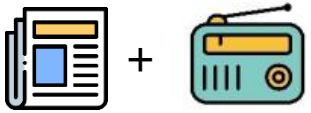
Conduire une étude de veille technologique sur le recours aux techniques de scoring et l'utilisation de l'intelligence artificielle à des fins de lutte contre la fraude

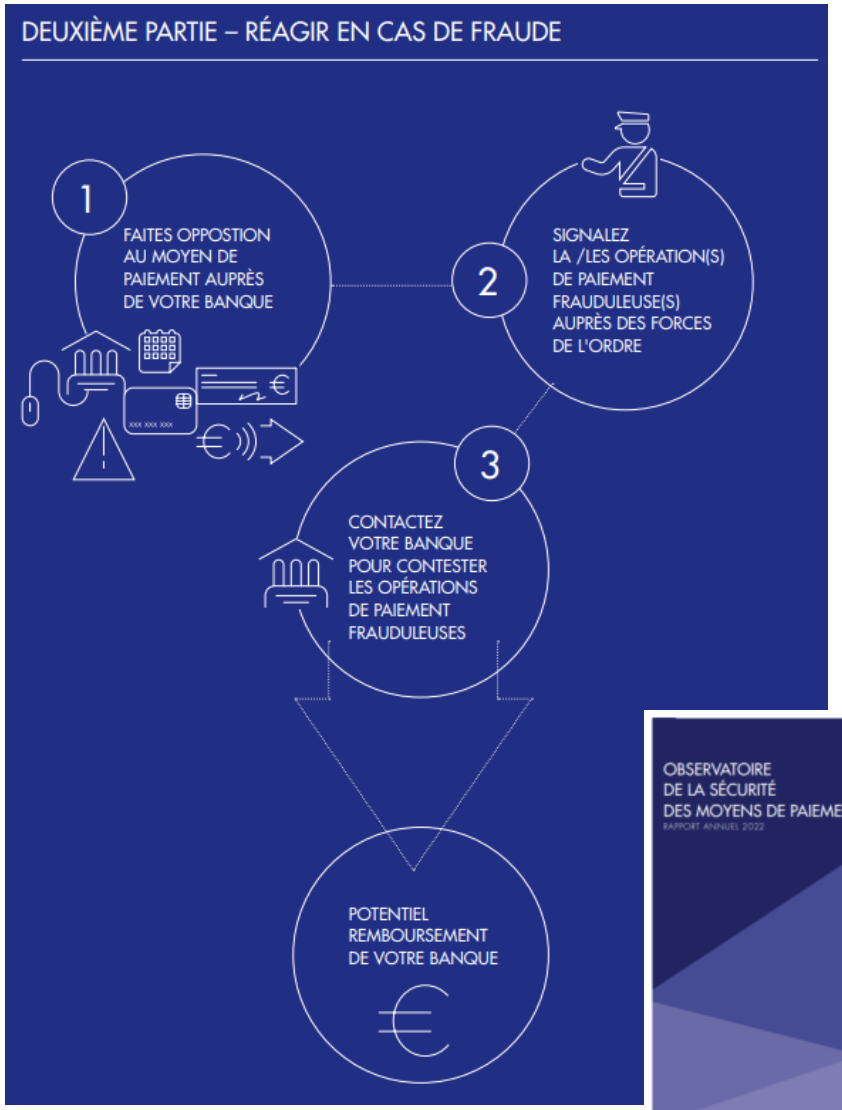
Établir un premier bilan à 18 mois des recommandations adoptées en mai 2023 par l'Observatoire sur le remboursement des cas de fraude

- Communication publique des résultats au plus tard début 2025
- Action d'évaluation confiée au superviseur bancaire

ACPR
BANQUE DE FRANCE

La sensibilisation des utilisateurs, une priorité permanente de l'Observatoire





Présentation du 8e rapport annuel

par Denis Beau, Président
et Julien Lasalle, Secrétaire

Conférence de presse du 10 septembre 2024

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