Présentation du 7e rapport annuel

par François Villeroy de Galhau, Président et Julien Lasalle, Secrétaire

Conférence de presse du 11 juillet 2023

Observatoire de la sécurité des moyens de paiement

www.observatoire-paiements.fr

Plan de la présentation

1) Bilan statistique de l'année 2022

- L'évolution des paiements scripturaux
- L'état de la fraude aux moyens de paiement

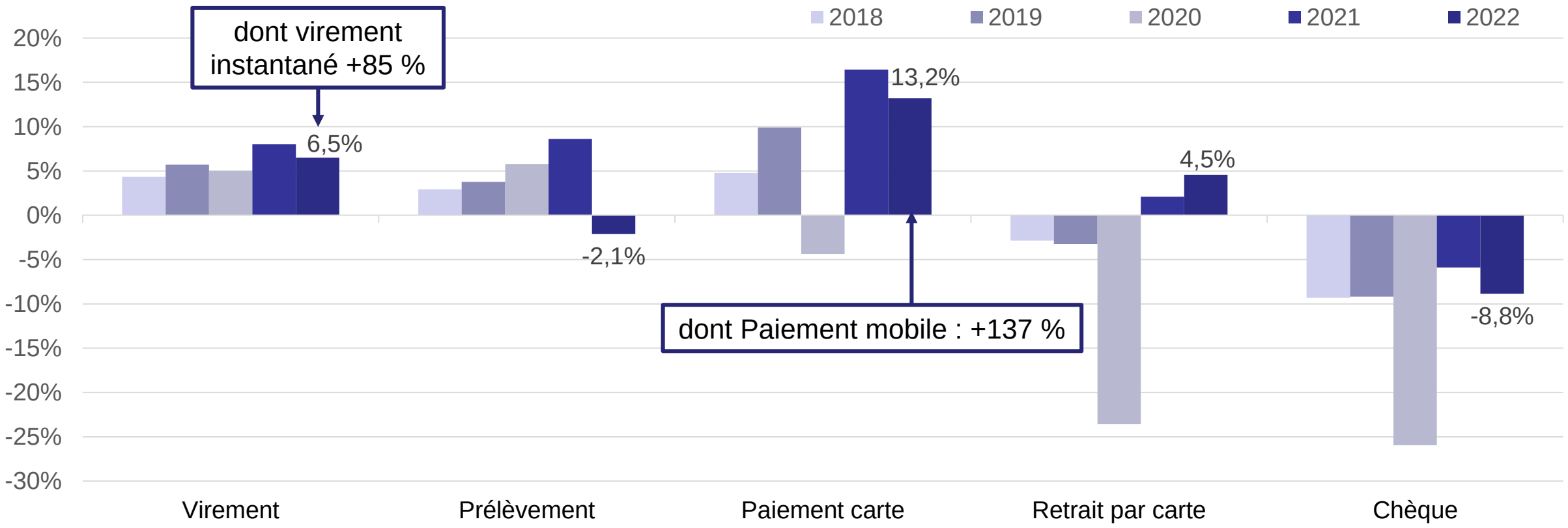
2) L'action de l'Observatoire

- Le bilan de l'authentification forte pour les paiements par carte sur Internet
- Le remboursement des victimes de fraude
- La sécurité des *smartphones* comme terminaux d'acceptation
- Le suivi des actions sur le chèque

Une croissance globale des paiements scripturaux en 2022

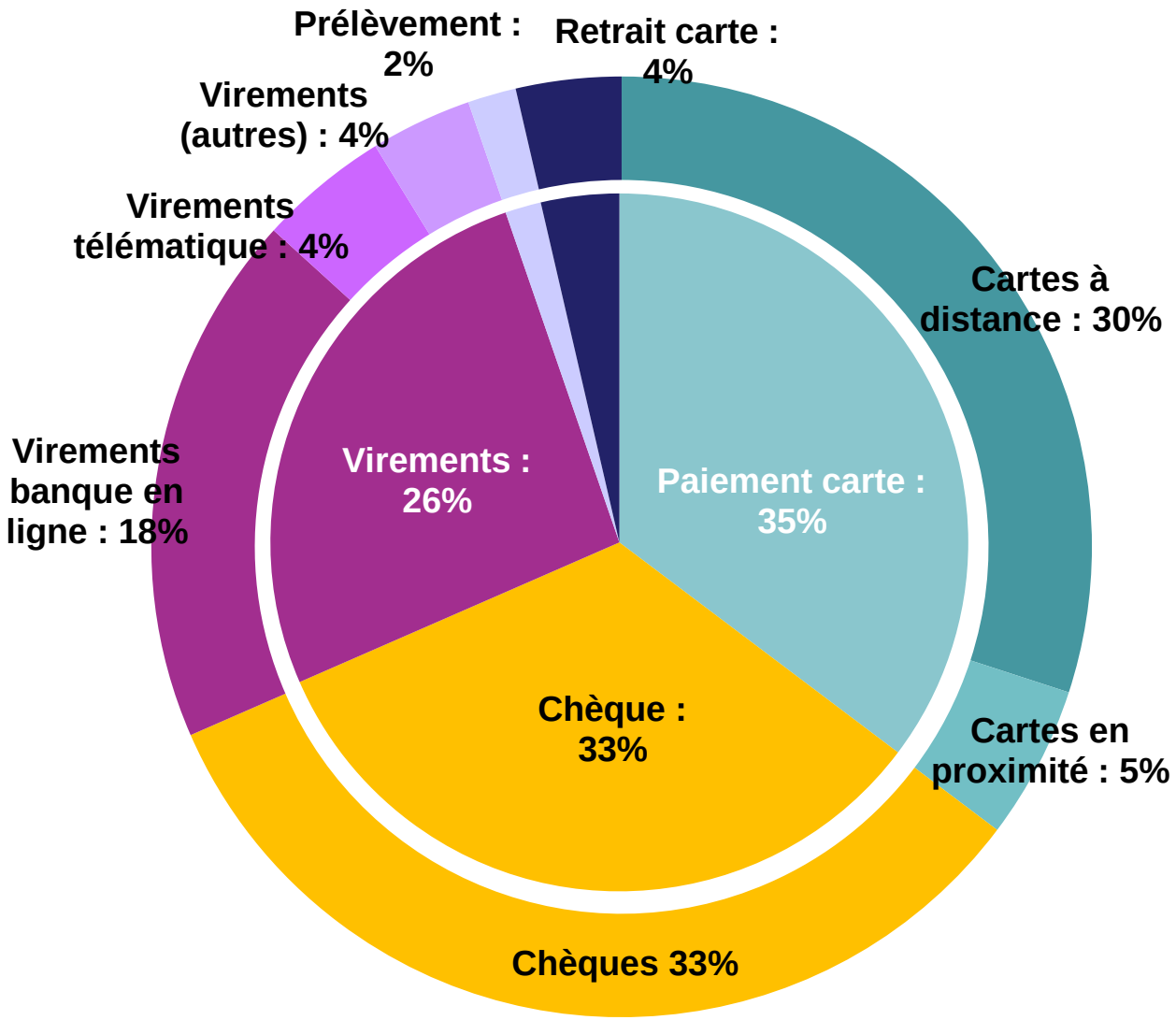
Évolution annuelle des flux de paiement (en volume)

Au global : 31 milliards d'opérations (+8 % en volume) / 42 578 milliards d'euros (+1 % en montant)



État de la fraude – Vue d'ensemble

Répartition de la fraude en valeur

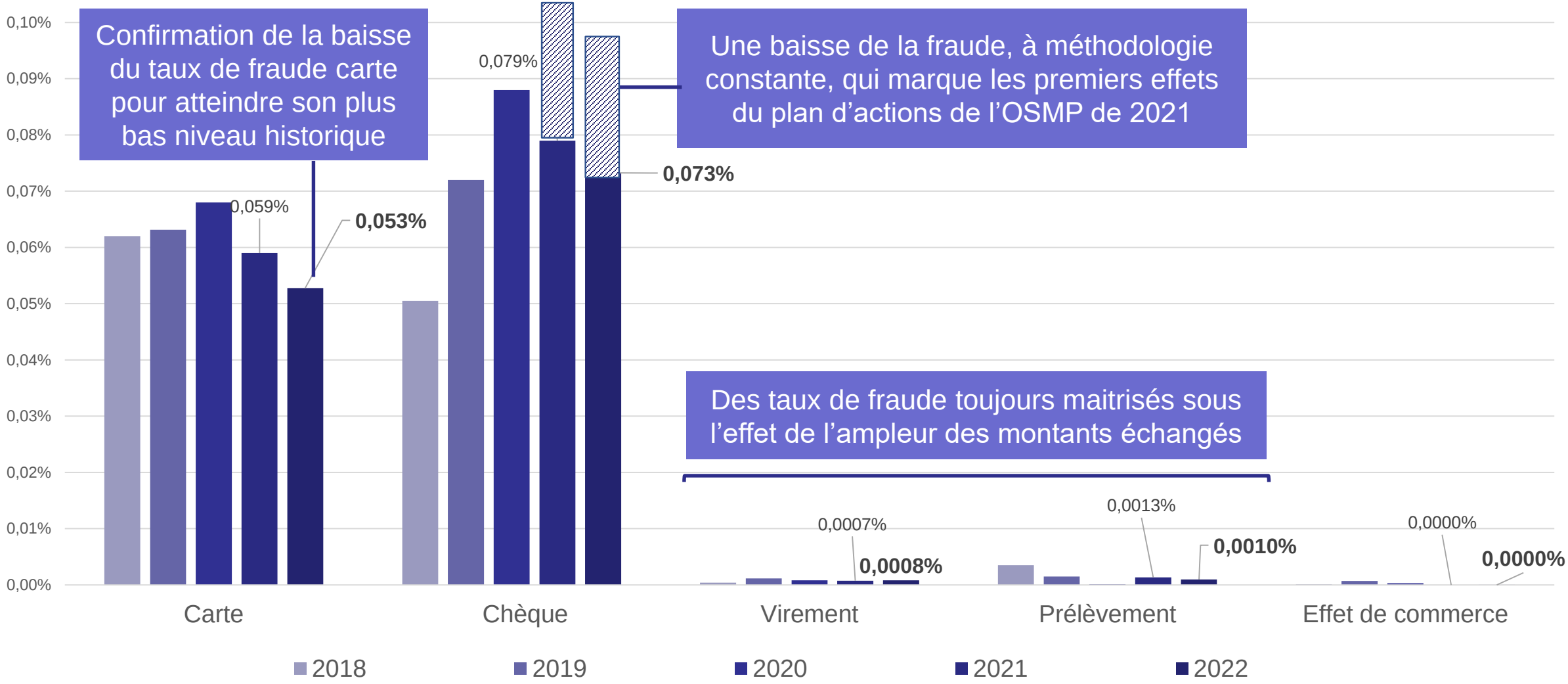


Total de la fraude = 1,19 Md € / 7,2 millions de transactions frauduleuses
(-4 % par rapport à 2021
en volume et en valeur)

- Pour les moyens de paiement électroniques, les **canaux d'utilisation à distance** restent les principales cibles des fraudeurs
- Le développement des **techniques de manipulation** touchant les particuliers, notamment l'usurpation d'identité du personnel bancaire par téléphone

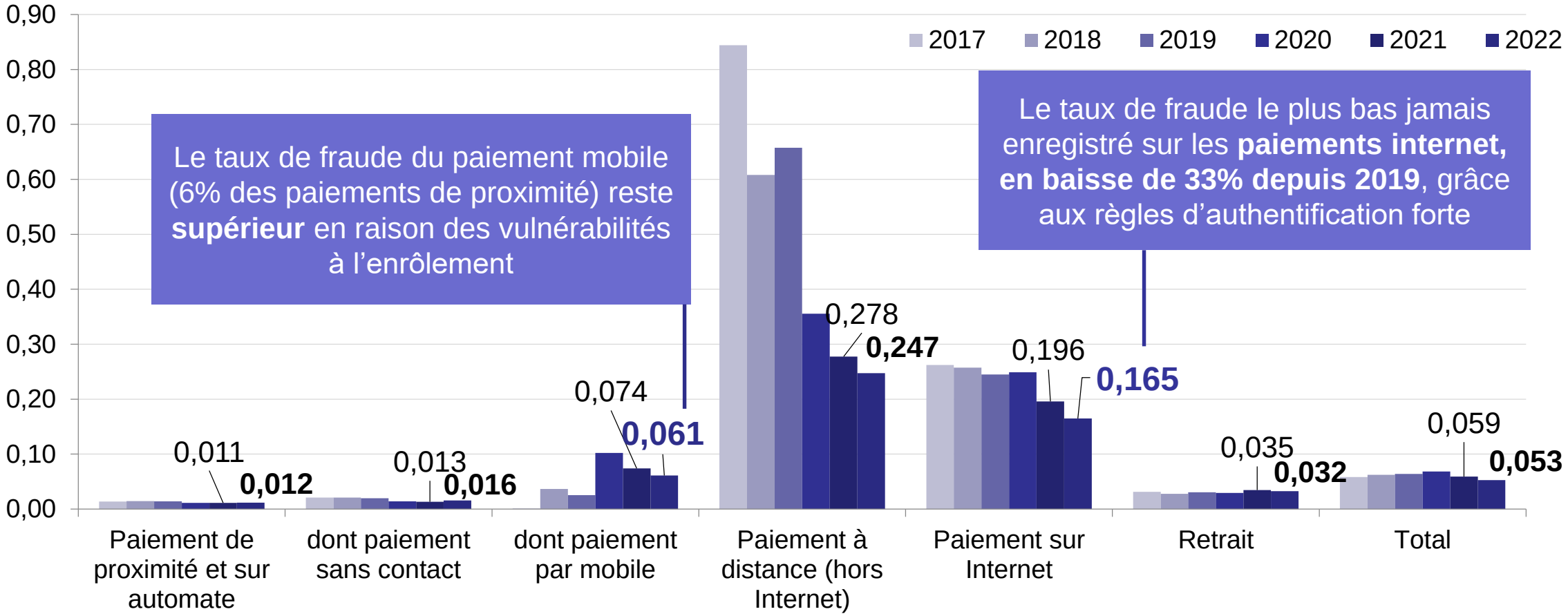
L’évolution des taux de fraude

Évolution des taux de fraude par instrument (en valeur)



Une baisse du taux de fraude sur la carte

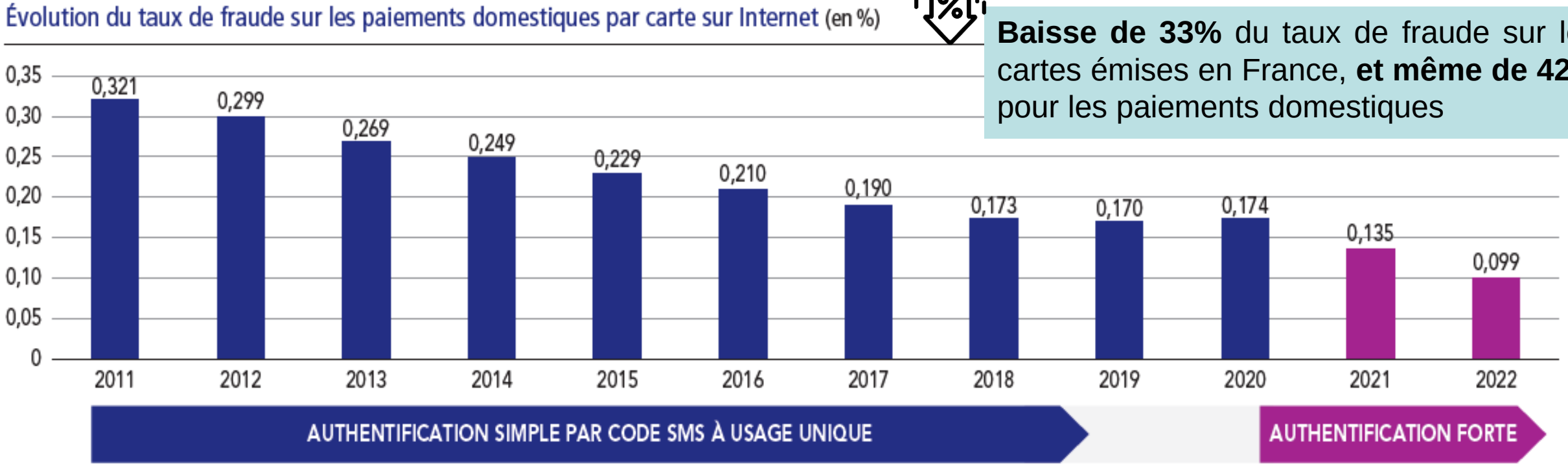
Évolution des taux de fraude par canal d'initiation (%, en valeur)



Part des flux en montant	**61 %**	***dont 15 %***	***dont 2 %***	**2 %**	**22 %**	**15 %**

Focus sur la fraude à la carte sur internet

Une baisse importante du taux de fraude depuis 2019



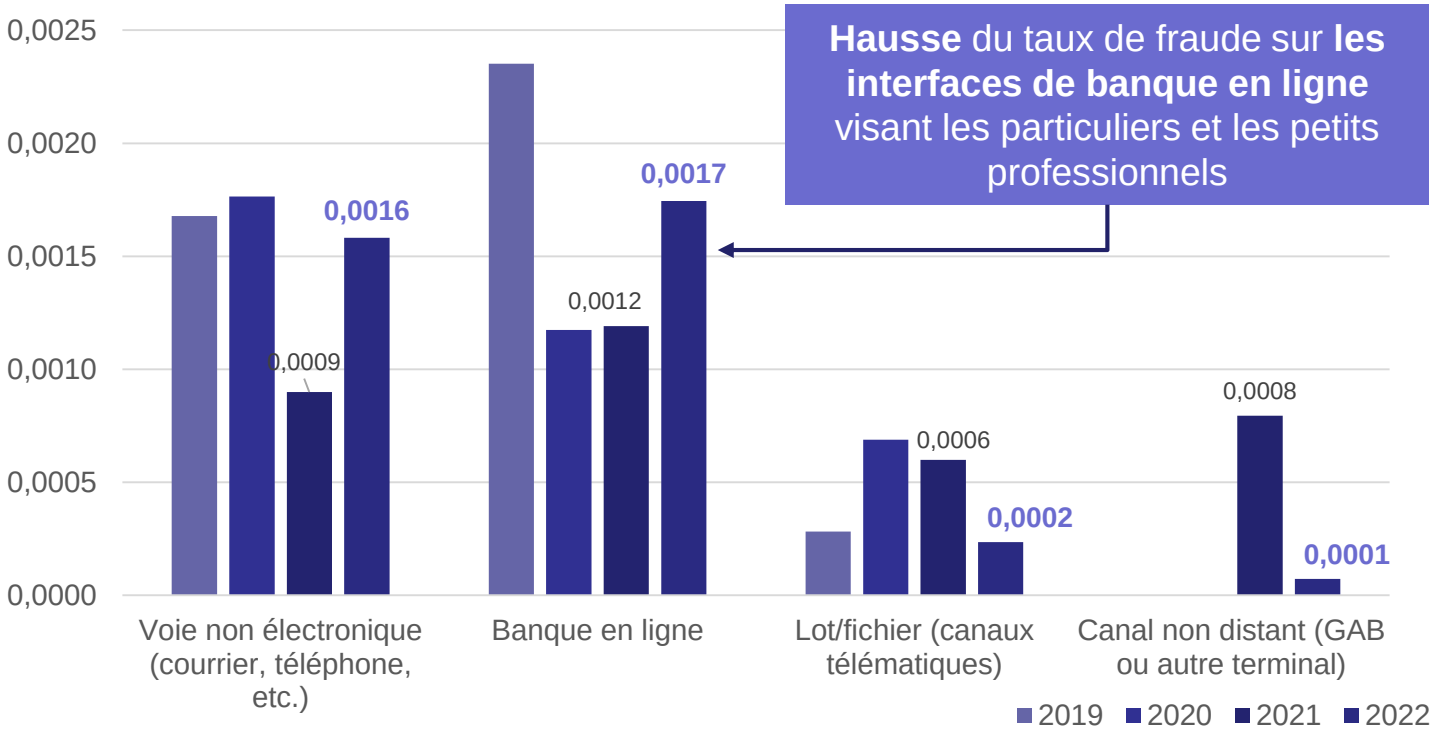
Source : Observatoire de la sécurité des moyens de paiement.

Baisse de 33% du taux de fraude sur les cartes émises en France, **et même de 42%** pour les paiements domestiques

Une hausse de la fraude sur le virement

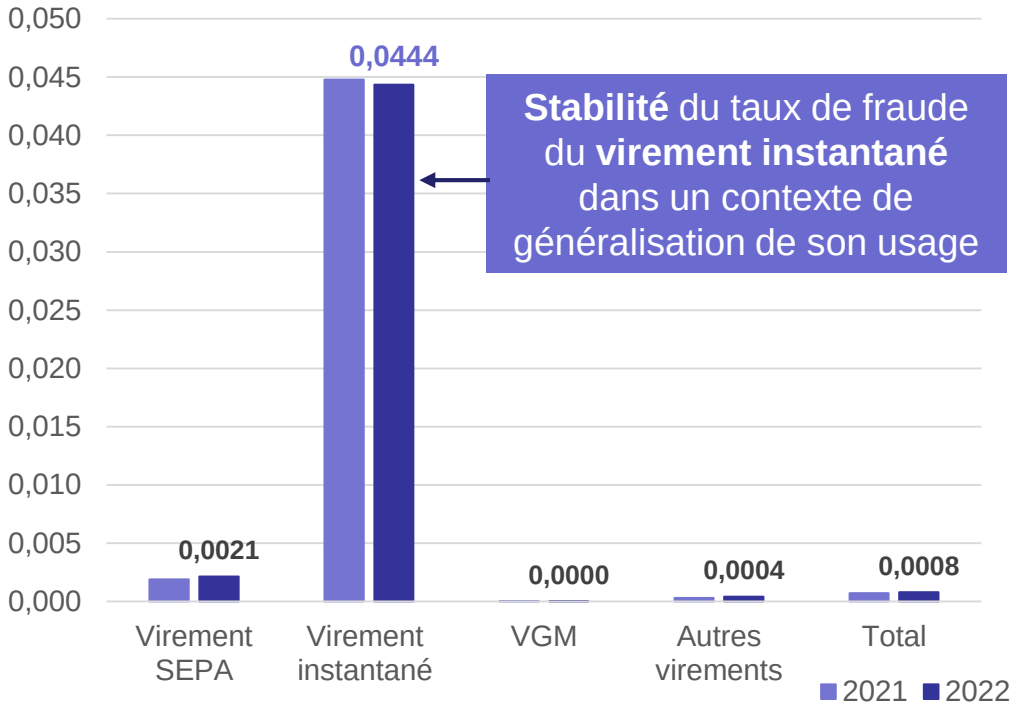
L'évolution des taux de fraude sur le virement (%, en valeur)

Évolution du taux de fraude sur virement par canal d'initiation (en %)



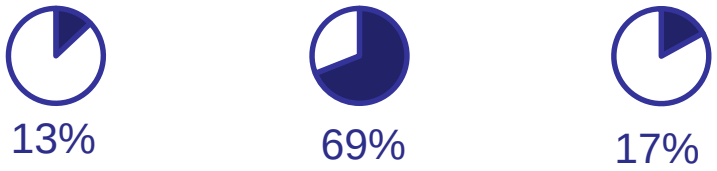
Hausse du taux de fraude sur **les interfaces de banque en ligne** visant les particuliers et les petits professionnels

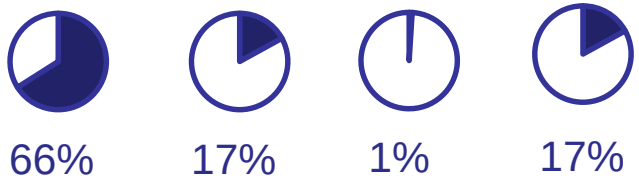
Taux de fraude par type de virement (en %)



Stabilité du taux de fraude du **virement instantané** dans un contexte de généralisation de son usage

Part de la fraude en valeur en 2022





Plan de la présentation

1) Bilan statistique de l'année 2022

- L'évolution des paiements scripturaux
- L'état de la fraude aux moyens de paiement

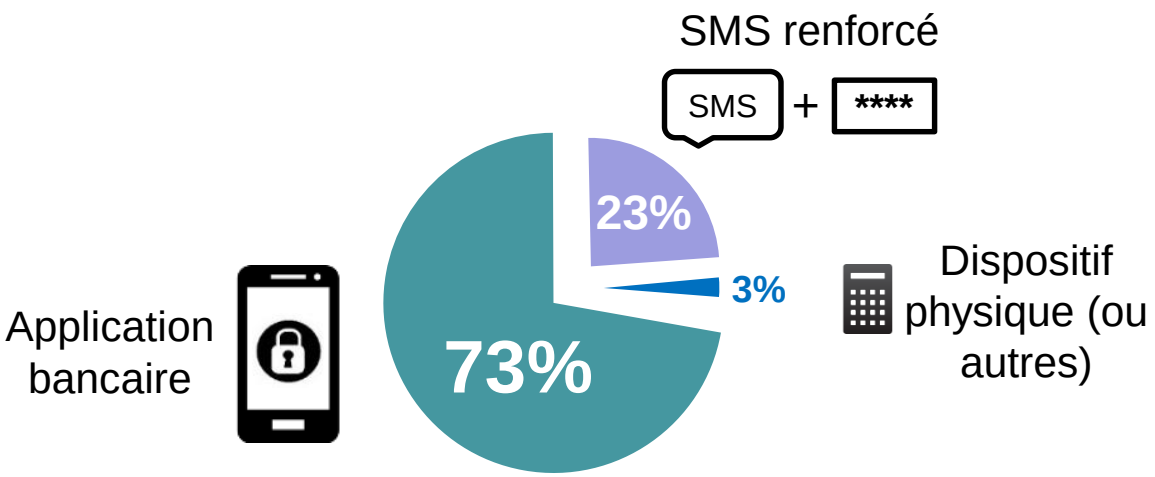
2) L'action de l'Observatoire

- Le bilan de l'authentification forte pour les paiements par carte sur Internet
- Le remboursement des victimes de fraude
- La sécurité des *smartphones* comme terminaux d'acceptation
- Le suivi des actions sur le chèque

Notre action (1) : Paiements par carte sur internet

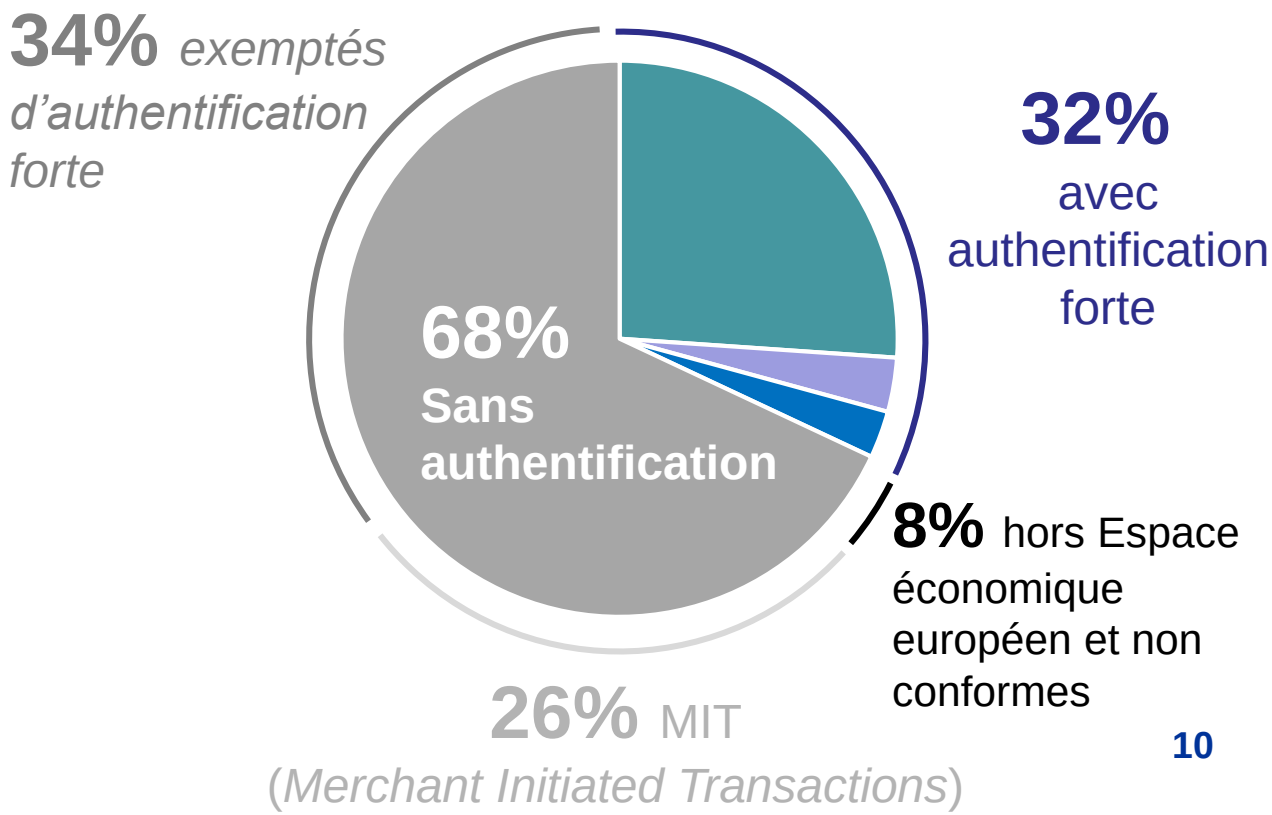
Aperçu des usages après la mise en œuvre des règles d'authentification forte

L'application bancaire, jugée techniquement plus sûre que le SMS renforcé, gagne du terrain (+5 points) dans l'équipement des porteurs…



… mais liberté de choix des utilisateurs avec disponibilité d'une méthode alternative et gratuite à l'application bancaire

En volume, les paiements sans authentification forte restent majoritaires, en raison des paiements exemptés ou exclus de l'authentification forte

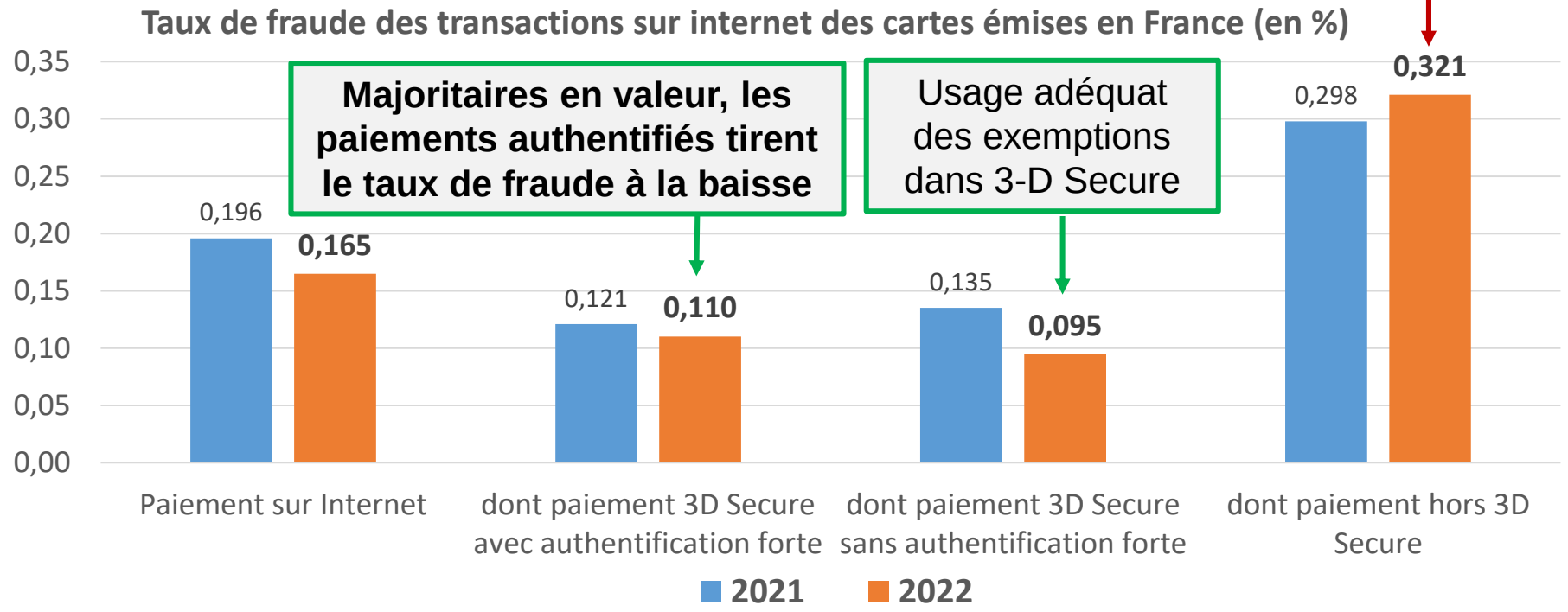


Notre action (1) : Paiements par carte sur Internet

Des marges de progrès supplémentaires

Canaux plus exposés à la fraude

Recommandations



Majoritaires en valeur, les paiements authentifiés tirent le taux de fraude à la baisse

Usage adéquat des exemptions dans 3-D Secure

	Paiement sur Internet	dont paiement 3D Secure avec authentification forte	dont paiement 3D Secure sans authentification forte	dont paiement hors 3D Secure
Part des flux <u>en valeur</u> 2022	59%	14%	27%
Part de la fraude <u>en valeur</u> 2022	39%	8%	53%

1) Sécuriser les « prélèvements » (MIT) par une authentification forte du mandat

2) Surveiller les exemptions hors 3-D Secure

3) Refuser les paiements sans motifs d'exemption

IMPORTANT

Lignes directrices pour l'exemption fondée sur le *scoring* de la transaction

Notre action (2) : Le remboursement des victimes de fraude

De nouveaux procédés frauduleux pour contourner l'authentification forte

Des **fraudes par manipulation** exploitant différentes techniques…
- Spoofing
- Phishing/smishing
- Accès aux comptes

… pour convaincre la victime de **valider des opérations à son insu**

Des fraudes qui ont touché en 2022 à la fois les **virements de banque en ligne (env. 2/3)** et les **paiements par carte sur Internet (env. 1/3)**

Un préjudice estimé à au plus **342 millions €**

Une part en hausse **7 points** (de 22 à 29%) dans une fraude globalement en baisse

---

Des **difficultés rencontrées par les victimes pour faire valoir le droit à remboursement en cas de fraude** prévu par la réglementation

➔ Authentification forte souvent considérée comme une présomption d'autorisation de la transaction ou de négligence grave, voire de comportement frauduleux

Notre action (2) : Le remboursement des victimes de fraude

Treize recommandations pour améliorer le remboursement des victimes et renforcer la lutte contre la fraude (*publiées en mai dernier*)

Application du droit à remboursement

Remboursement immédiat des opérations effectuées sans authentification forte, y.c. les paiements par solution mobile sans authentification forte à l'enrôlement

L'authentification forte ne justifie pas à elle seule un non remboursement et nécessite d'**analyser un ensemble plus large de critères pour statuer**

Outils de prévention de la fraude

Exiger une authentification forte en cas de consultation des comptes en ligne depuis un nouveau terminal

Indiquer de façon explicite la **nature des contrôles réalisés lors de la saisie de l'IBAN et le nom du titulaire du compte** lors de l'ajout d'un bénéficiaire de virement

Engagements des acteurs

Protéger leurs utilisateurs contre les risques d'usurpation d'identité et d'atteinte à l'intégrité et la confidentialité de leurs données **au niveau des réseaux télécom**

Entrée en application de la loi Naegelen le 25 juillet prochain contre les appels frauduleux

Notre action (3): La sécurité des smartphones comme terminaux

Les innovations dans les terminaux depuis 10 ans

Terminaux autonomes et mobiles (4G)

Terminaux m-POS associé à un smartphone

Terminaux Android

Solutions SoftPOS (*Software Point of Sale*)

Accompagnée par une évolution des normes de sécurité de l'industrie des paiements par carte (*Payment Card Industry*, PCI)

2018

SPoC (Software-based PIN entry on COTS)

2019

CPoC (Contactless Payments on COTS)

2022

MPoC (Mobile Payments on COTS)

* POS: *Point of Sale*, point de vente ; COTS: *Commercial Off-The-Shell*, produit informatique grand public

Notre action (3): La sécurité des smartphones comme terminaux

Les recommandations de l'Observatoire

Objectif: préserver absolument le très haut niveau de sécurité des paiements par carte de proximité sans empêcher l'innovation

1 – Fournisseurs et industriels des paiements

- ✓ Assurer **la confidentialité et l'intégrité** des données de carte et du code confidentiel de bout-en-bout
  - avant lancement: obtenir toutes les certifications nécessaires
  - après lancement: déployer un programme de contrôle
- ✓ **Sélection prudente et rigoureuse** des environnements de déploiement

2 – Commerçants utilisateurs

- ✓ **Porter la même attention** aux smartphones qu'aux terminaux « traditionnels » (mises à jour, installation des applications tierces, sécurité physique avec signe distinctif…)
- ✓ Prévoir une **solution alternative** adaptée aux utilisateurs souffrant de **handicap visuel**

Notre action (4) : suivi du plan de 2021 contre la fraude au chèque

Des améliorations, mais des progrès encore attendus

Des **mécanismes bancaires de surveillance et de temporisation** des encaissements de chèque, dont l'efficacité progresse pour déjouer les escroqueries
> 161 millions d'euros de fraude déjouée soit 29% des tentatives de fraude

Une modernisation du **service officiel VÉRIFIANCE** pour élargir la consultation du Fichier national des chèques irréguliers (FNCI) aux **particuliers et professionnels**, par l'intermédiaire de leur banque mandataire

Sécurisation perfectible des **envois de chéquiers par voie postale** (environ 2/3 de la distribution), les clients devant garder explicitement la possibilité de retirer leur chéquier **gratuitement en agence**

Des progrès attendus dans la simplicité et l'accessibilité des **procédures de mise en opposition**, dans leurs dimensions pratique et tarifaire

Présentation du 7e rapport annuel

par François Villeroy de Galhau, Président et Julien Lasalle, Secrétaire

Conférence de presse du 11 juillet 2023

Observatoire de la sécurité des moyens de paiement

www.observatoire-paiements.fr