- PUBLIC -

Fraude aux moyens de paiement

Évolutions récentes et mesures de prévention

3 février 2022

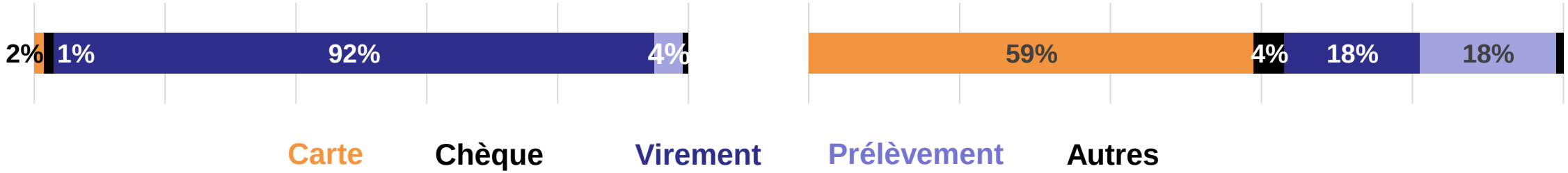
Observatoire
de la sécurité
des moyens de paiement

www.observatoire-paiements.fr

Données statistiques du 1er semestre 2021

Vue d'ensemble

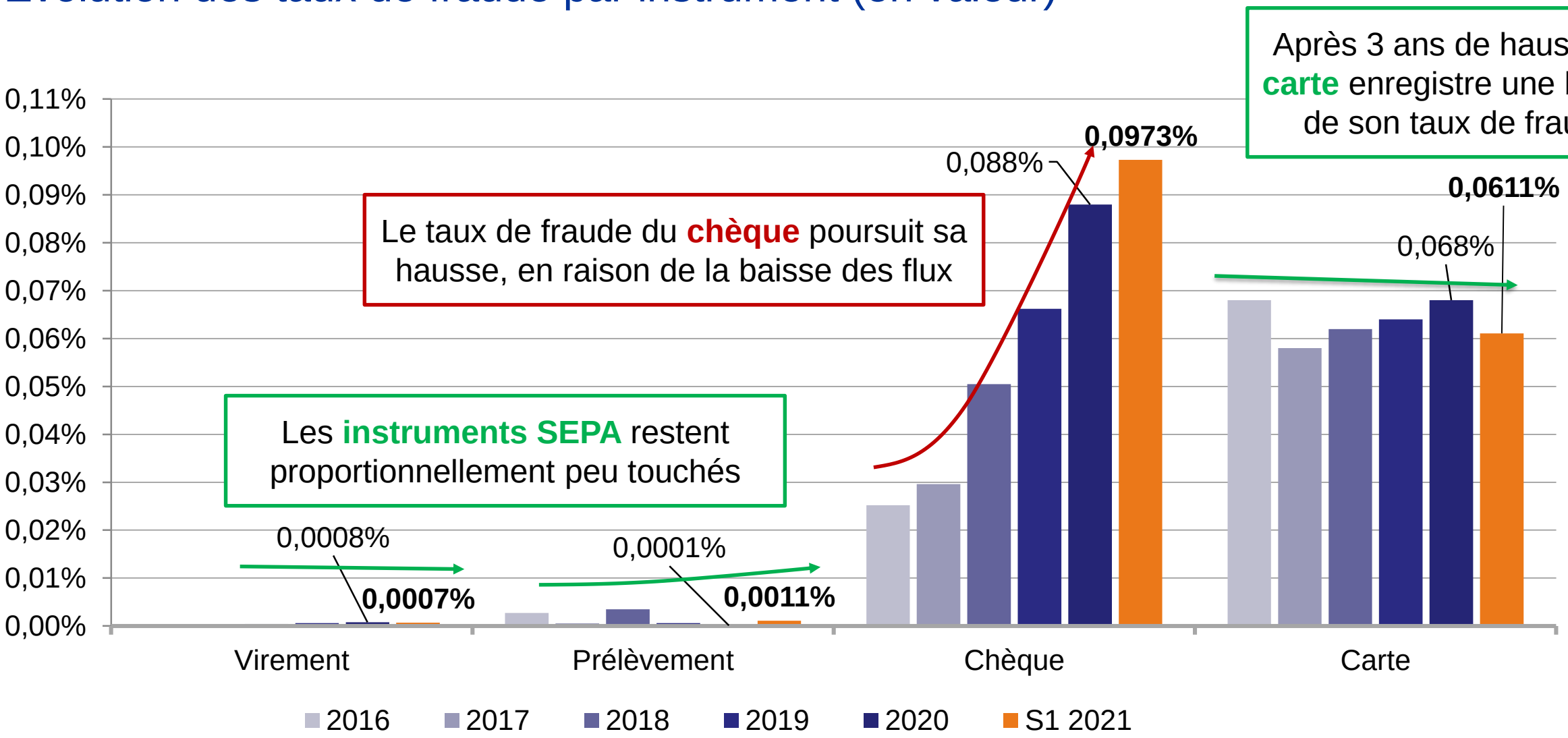
20 504 milliards d'euros échangés pour **13,2 milliards de transactions**



… et une fraude de l'ordre de
644 millions d'euros pour **3,6 millions de cas**

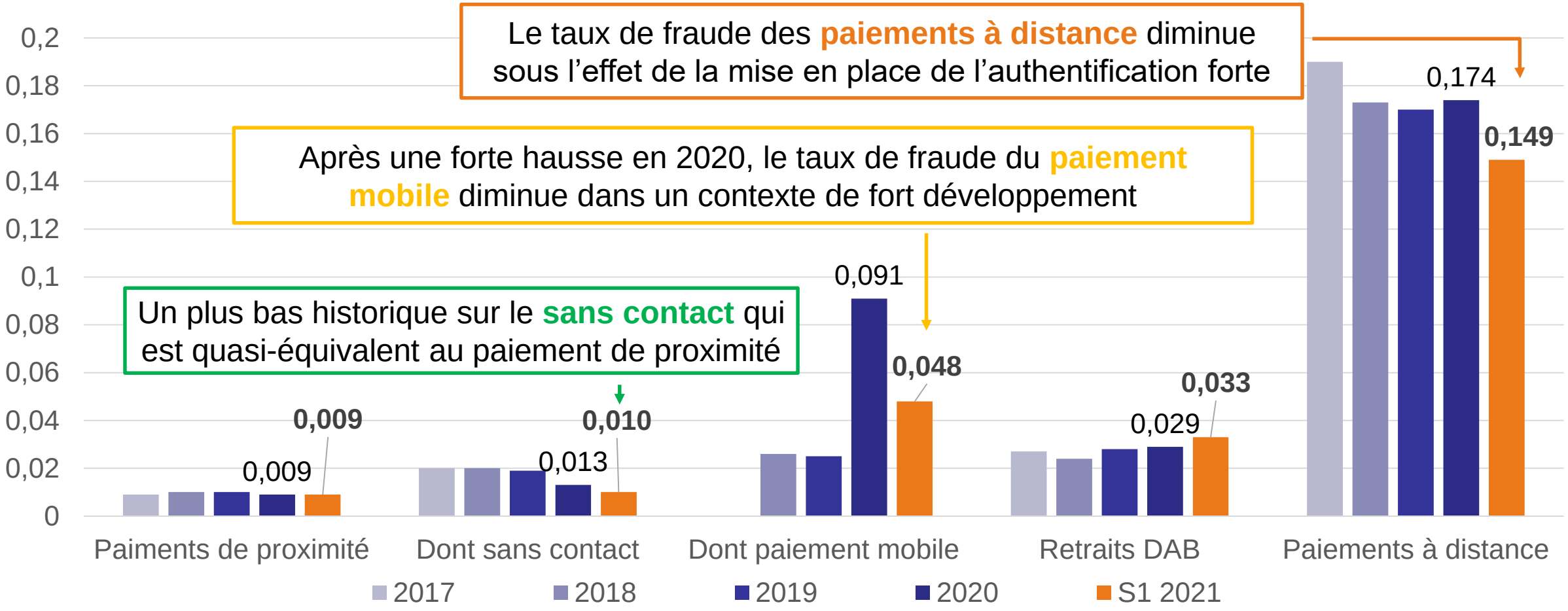
L'évolution des taux de fraude au 1er semestre 2021

Évolution des taux de fraude par instrument (en valeur)



L'évolution des taux de fraude sur la carte au 1er semestre 2021

Par canal d'initiation pour les transactions domestiques (%, en valeur)

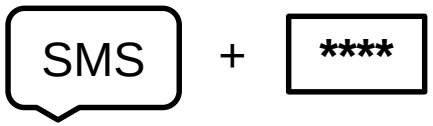


Un bilan très positif du déploiement de l'authentification forte à fin 2021

>97% des porteurs actifs sur internet enrôlés dans un **dispositif d'authentification forte**

- soit une application bancaire sécurisée

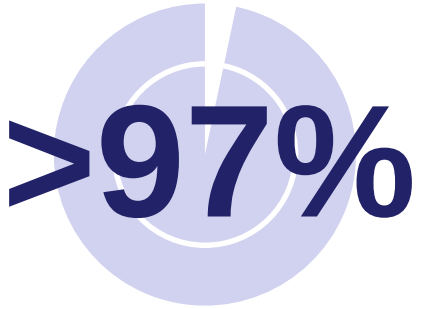
- soit un dispositif de SMS/SVI renforcé



- soit un boitier physique dédié

➔ Les banques sont tenues de proposer à leurs clients et sans surcoût au moins une solution alternative à l'application mobile

Un bilan très positif du déploiement de l'authentification forte à fin 2021



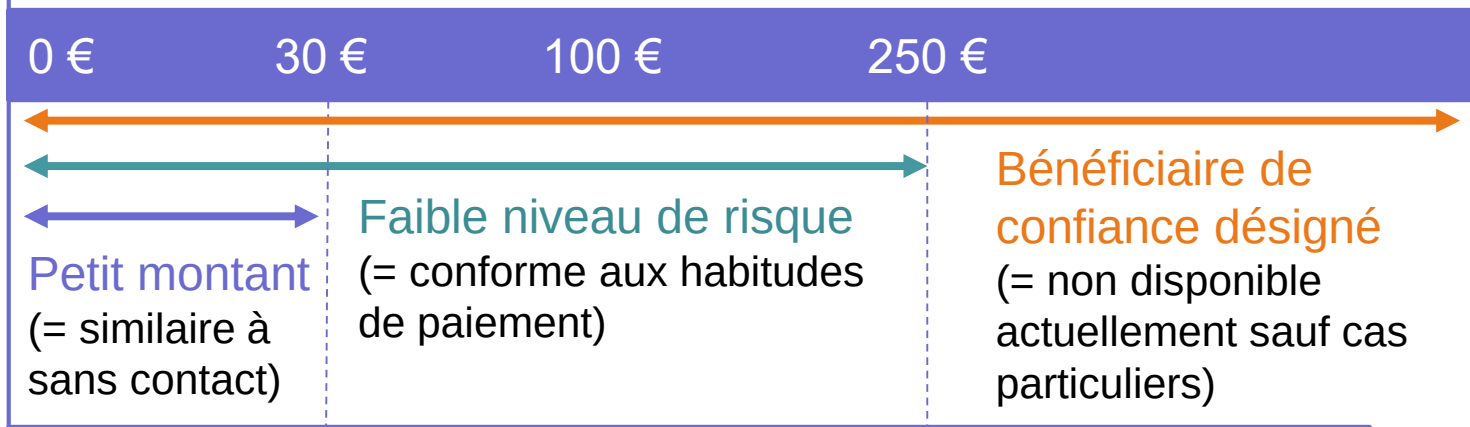
>97% des flux en valeur émis par les commerçants **conformes aux obligations réglementaires**

- soit l'appel à une authentification forte du payeur via 3D-Secure

3DS

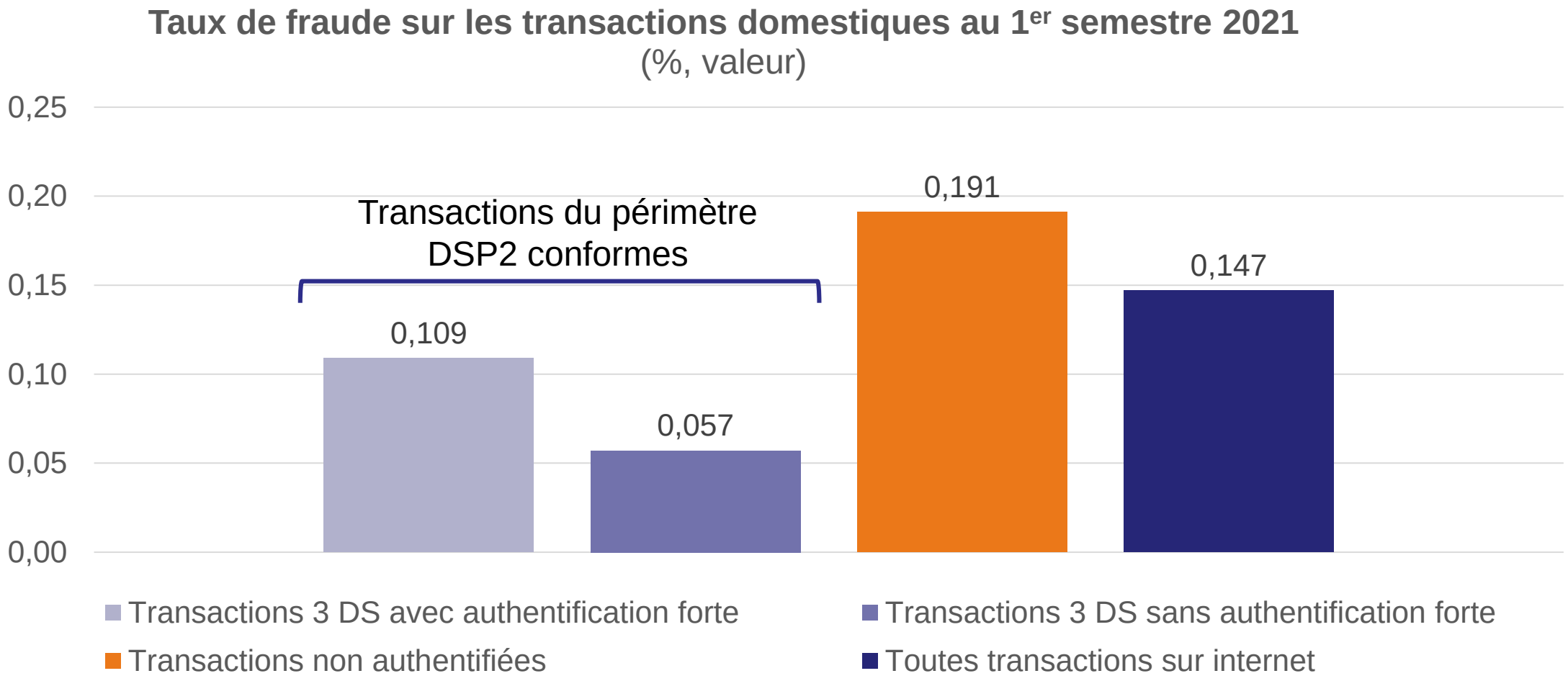
- **Obligatoire** pour toute souscription à un paiement récurrent, fractionné ou différé
- **Recommandé** à chaque fois que la carte est enregistrée dans un espace client ou une application mobile

- soit l'application d'une exemption permettant un paiement sans authentification forte



Quel que soit le type d'exemption, l'absence d'authentification forte doit être approuvée par la banque du porteur

Des premiers résultats prometteurs sur le risque de fraude



De nouveaux types de fraude qui visent à contourner l'authentification forte en manipulant le porteur

1

Le fraudeur **collecte des données** sur sa cible:

- Attaques informatiques (*phishing, malware, dark web*…)
- Recherche sur les réseaux sociaux

2

Le fraudeur **contacte en direct** sa cible :

- en se faisant passer pour sa banque (*spoofing*)
- prétexte une transaction frauduleuse ou une tentative de fraude
- prétend devoir réaliser un test de sécurité ou des opérations d'annulation pour protéger l'utilisateur

3

La cible est invitée à **valider des opérations via ses moyens d'authentification** :

- paiement unitaire par carte
- ajout d'un bénéficiaire et émission d'un virement (instantané)
- modification du plafond de paiement ou de découvert autorisé
- enrôlement de la carte dans une solution de paiement mobile
- transfert du moyen d'authentification forte

➔ Via ce type d'attaque, le fraudeur amène sa victime à valider à son insu des opérations frauduleuses en passant outre les différentes alertes adressées par la banque

Face à ces nouvelles techniques de fraude, la vigilance des consommateurs est un rempart essentiel

Ne répondez pas aux sollicitations des fraudeurs

- **Utilisez toujours un canal sécurisé et connu** (favori, moteur de recherche) **pour vous connecter à votre banque**, ne cliquez jamais sur un lien reçu par mail ou SMS
- **Refusez toute communication non sollicitée** qui vous serait proposée en direct (téléphone, chat…) et recontactez votre banque par votre canal habituel

Utilisez à bon escient vos outils et données d'authentification

- Vos outils et données d'authentification sont **aussi sensibles que le code de votre carte**
- Ne les utilisez que pour **des transactions dont vous êtes l'auteur** et **ne les communiquez jamais à un tiers**
- Votre banque ne vous demandera **jamais** de valider à distance une opération à des fins de test ou en réponse à une fraude