FRAUDE AUX MOYENS DE PAIEMENT :
Comment les recommandations de l'OSMP* impactent les banques ?

Publié en juillet 2023, il présente l'état des lieux des **moyens de paiement et de la fraude en France en 2022**

Depuis le début de la pandémie, **l'utilisation des moyens de paiement électroniques a continué de croître**. On constate une augmentation de 8 % sur l'année 2022. L'utilisation de la carte sans contact en paiement de proximité est de plus en plus populaire ; elle représente désormais plus de six paiements sur dix. Le **paiement par carte sur mobile a également explosé** (+137 %) tandis que le virement instantané a augmenté de 85 %.

Malgré cette croissance, la **fraude a reculé de 4 %** en volume et en valeur, atteignant 1,19 milliard d'euros. Les cartes de paiement ont enregistré **un taux de fraude historiquement bas pour ces moyens de paiements** (0,053%) grâce à des améliorations de sécurité. En parallèle, les paiements mobiles en proximité restent vulnérables en raison de faiblesses dans les processus d'enregistrement, avec un taux relativement élevé (0,061%).

Les chèques ont vu leur fraude diminuer mais demeurent les plus exposés. Les virements ont connu une hausse de la fraude, principalement depuis les interfaces de banque en ligne, touchant les particuliers et les petites entreprises.

Ce rapport, qui fait suite aux dispositions mises en œuvre dans le cadre de la DSP2, émet des recommandations à destination des banques, des porteurs de carte et des fournisseurs de services et technologies de l'information pour **améliorer le remboursement des victimes de fraude et renforcer la sécurité des paiements en ligne**.

Il souligne la nécessité de prudence lors de l'utilisation de terminaux grand public pour les paiements par carte.

Enfin, l'Observatoire s'**engage à maintenir la sécurité des moyens de paiement** dans un contexte en constante évolution et à collaborer avec les opérateurs télécoms pour prévenir l'usurpation d'identité et lutter contre la fraude.

Le Rapport complet

capteo

**Observatoire de la Sécurité des Moyens de Paiement*

RECOMMANDATIONS GENERALES APPLICABLES AU TRAITEMENT DES **CONTESTATIONS D'OPERATIONS DE PAIEMENT**

Délais maximums d'investigation

Recommandation 01

Signification

Investigation sous 30 jours maximum sauf situation exceptionnelle*

Conséquences

Aujourd'hui, il n'y pas de délais demandés aux banques.

Les délais d'investigation puis des échanges pour finaliser une analyse est variable et dépasse souvent 30 jours simplement pour avoir une réponse d'un schème ou d'une banque confrère.

Information du client en cas de reprise des fonds

Recommandation 02

Signification

Information au client sur la reprise possible des fonds suite aux investigations dans un délai de 30 jours maximum à compter de la date du remboursement, sauf situation exceptionnelle*

Conséquences

Aujourd'hui, il n'y a pas de délais stipulés dans la loi pour reprendre les fonds. Les banques devront alors s'organiser en mettant en place des rappels en fonction des dates de remboursement et/ou mettre en place de nouvelles procédures.

Justification du refus de remboursement

Recommandation 03

Signification

Indication du motif détaillé ainsi que les modalités pour déposer une réclamation du refus ou la reprise de fonds.

Conséquences

Aujourd'hui, la réponse est souvent large, en indiquant simplement que la banque ne rembourse pas car la demande ne répond pas à la législation.

Dans le futur, les banques devront faire une réponse détaillée avec les données techniques, l'opération contestée et le motif de refus en lien avec la législation.

capteo

**Observatoire de la Sécurité des Moyens de Paiement*

RECOMMANDATIONS APPLICABLES AU TRAITEMENT DE **CAS SPECIFIQUES**

Recommandation

Principes applicables aux opérations sans authentification forte

04

Signification

Remboursement automatique et immédiat d'une contestation d'opération sans authentification forte sauf en cas de soupçon de fraude de la part de l'utilisateur.

Conséquences

Aujourd'hui, l'intégralité des paiements n'est pas effectuée avec authentification forte. La majorité des paiements validés par ce biais s'effectue via Internet (VAD). La Banque de France préconise le remboursement lorsqu'il s'agit d'un prélèvement ou lorsque le paiement est effectué par carte et que le bénéficiaire n'indique pas les données de paiement.

Recommandation

Principes applicables aux opérations réalisées avec une application mobile se substituant à l'instrument de paiement

05

Signification

Remboursement immédiat d'une contestation d'opérations effectuées via une solution mobile sans authentification forte

Conséquences

Aujourd'hui, l'enrôlement d'un instrument de paiement par ce biais ne nécessite pas d'authentification forte. Si celle-ci n'est pas mise en place, les banques seront dans l'obligation d'effectuer le remboursement à J+1.

Recommandation

Principes applicables aux operations authentifiees de maniere forte

06

Signification

Première analyse technique, de contexte et de modalité à effectuer à J+1 dans le cas de contestation d'opérations de paiement authentifiées de manière forte.

Conséquences

Aujourd'hui, la règle est de ne jamais rembourser le client s'il y a authentification forte. Contraindre la banque à une première analyse à J+1 va imposer une mise en place d'importants changements pour réduire ces délais en termes de procédures au niveau des équipes et des automatisations.

RECOMMANDATIONS A L'**ATTENTION DES CONSOMMATEURS ET DE LEURS REPRESENTANTS**

Recommandation **07**

BONNES PRATIQUES POUR LA SECURITE DES MOYENS DE PAIEMENT

Signification
Appel à la vigilance des consommateurs sur la préservation des données de paiements

Conséquences
Pas d'impact côté banque

Recommandation **08**

DEVOIR DE TRANSPARENCE DE LA PART DES VICTIMES DE FRAUDE

Signification
Obligation des consommateurs de fournir les détails pertinents sur l'opération frauduleuse.

Conséquences
Pas d'impact côté banque

RECOMMANDATIONS VISANT A **PREVENIR DE LA FRAUDE** *(1/2)*

Recommandation **09**

Application d'une authentification forte lors de l'accès à la banque en ligne depuis un nouveau point d'accès à internet ou un nouveau terminal

Signification
Mise en place d'une authentification forte en cas de connexion sur un nouveau terminal.

Conséquences
Aujourd'hui, les authentifications fortes sont souvent demandées. Si non, cela générera des impacts techniques (en termes de développement et de traçabilité).

Recommandation **10**

Modalités d'enregistrement des IBAN bénéficiaires de virements

Signification
Indication du contrôle de concordance IBAN/bénéficiaire.

Conséquences
Aujourd'hui, aucune vérification n'est effectuée pour confirmer la concordance. Cela générera des impacts techniques : développement et implémentation du service de confirmation du bénéficiaire.

RECOMMANDATIONS VISANT A **PREVENIR DE LA FRAUDE** *(2/2)*

Recommandation **11**

Information et options présentées à l'utilisateur au moment de l'authentification forte

Signification

Présentation des conditions de sa transaction à chaque étape de validation (montant, bénéficiaire et caractère unique ou récurrent, périodicité).

Conséquences

Aujourd'hui, les données de transactions sont restituées à l'utilisateur lors de la première étape de validation. Là encore, des impacts techniques sont à prévoir : développement et implémentation de ces données à chaque étape d'acceptation de paiement.

Recommandation **12**

Simplicité d'accès aux procédures de blocage des instruments de paiement

Signification

Mise à disposition de mécanismes gratuits et facilement accessibles pour le blocage des instruments de paiement.

Conséquences

Aujourd'hui, des mécanismes de blocages sont déjà proposés par les banques pour les cartes. Il y aura un impact à prévoir pour les autres moyens de paiements : chèques, virements…

Recommandation **13**

Rôle des fournisseurs de services et technologies de l'information

Signification

Protection des utilisateurs contre l'usurpation de l'identité.

Conséquences

L'implication des acteurs des technologies de l'information est préconisée afin de protéger les utilisateurs.

CONCLUSIONS

Ces recommandations n'ont pas valeur législative et sont dans la continuité de la loi DSP2 européenne. Néanmoins, il est demandé aux banques françaises de les **mettre en application sans attendre avec pour échéance décembre 2023.**

En parallèle, de **nouvelles obligations** pour les émetteurs de **prélèvements SEPA** ont été émises en février 2023 ; ce rapport nous indique qu'une législation européenne serait à venir. Les montants de la fraude ayant augmenté en 2022 de 9%, **l'Observatoire lance des travaux dès septembre 2023** pour identifier les mesures complémentaires.