Recommandations sur le remboursement des victimes de fraude

22 mai 2023

COMMUNIQUÉ DE PRESSE

L'Observatoire de la sécurité des moyens de paiement émet des recommandations sur le remboursement des victimes de fraude

L'utilisation de mécanismes d'authentification forte du payeur, qui s'est généralisée depuis 2019 en application de la deuxième directive européenne sur les services de paiement (dite DSP2), a permis de réduire significativement la fraude aux paiements sur internet. La veille assurée par l'Observatoire montre ainsi que le taux de fraude sur les paiements par carte sur internet a baissé de 30% entre 2019 et 2022. L'Observatoire constate néanmoins que les fraudeurs cherchent à contourner l'authentification forte en développant de nouvelles techniques de fraude, qui s'appuient notamment sur la manipulation des victimes.

Face au développement de ces nouveaux procédés frauduleux qui touchent tous les profils de clients, l'Observatoire a souhaité apporterdes précisions sur le droit à remboursement prévu par la DSP2 en cas de fraude. **L'Observatoire publie à**

cette fin un ensemble de treize recommandations qui visent à améliorer les démarches de remboursement des victimes de fraude tout en rappelant la responsabilité des utilisateurs dans la sécurité de leurs moyens de paiement :

– Dès lors qu'une transaction contestée par le titulaire du compte n'a pas fait l'objet d'une
authentification forte, l'établissement teneur de compte est tenu de la lui rembourser sans délai, c'est-à-dire au plus tard à la fin du premier jour ouvré après réception de cette contestation ;

– Si une transaction contestée par l'utilisateur a fait l'objet d'une authentification forte, alors il revient à l'établissement teneur de compte de déterminer si cette transaction peut être considérée comme autorisée par l'utilisateur. Cette analyse doit s'appuyer sur les différents paramètres associés à la transaction (origine de la transaction, paramètres de l'authentification forte, interactions avec le payeur, etc.), l'existence d'une authentification forte n'étant pas suffisante en soi pour considérer que la transaction a été autorisée. Après analyse du dossier et à défaut d'éléments suffisants pour justifier le caractère autorisé de la transaction ou démontrer une négligence grave de l'utilisateur, l'établissement est tenu de rembourser sans délai l'opération en cause.

L'Observatoire assurera la diffusion de ces recommandations auprès des publics concernés ainsi qu'un suivi de leur mise en œuvre, avec l'appui de l'Autorité de Contrôle Prudentiel et de Résolution au titre de son mandat de contrôle des pratiques commerciales. Un premier bilan sera dressé à la fin de l'année 2024.

L'Observatoire rappelle également que la lutte contre la fraude requiert la vigilance de tous, et appelle l'ensemble des acteurs à s'approprier les recommandations qui les concernent et à adopter les meilleurs pratiques et comportements à cet égard :

– **Les consommateurs et les entreprises**, en étant toujours vigilants dans l'utilisation de leurs instruments de paiement et en veillant à la sécurité de leurs données, en privilégiant dans la mesure du possible la solution d'authentification forte la plus sûre et en faisant preuve de réactivité et de transparence en cas de fraude subie en vue de rapporter l'ensemble des éléments de contexte associés et

faciliter ainsi l'action des forces de l'ordre ;

– **Les prestataires de services de paiement**, en améliorant la clarté des notifications relatives aux opérations réalisées par leurs clients, en renforçant les contrôles effectués au moment de la validation d'opérations sensibles et en déployant des procédures de blocage accessibles et gratuites sur l'ensemble des instruments de paiement ;

– **Les autres acteurs de l'écosystème des paiements**, en premier lieu les acteurs du secteur de la téléphonie, en déployant des mécanismes de protection des attaques frauduleuses, en particulier au moment de l'émission de nouvelles cartes SIM, et de sécurisation des SMS et des appels téléphoniques.

L'Observatoire se félicite à ce titre de la campagne de sensibilisation lancée par la Fédération bancaire française dans les différents médias depuis le 22 avril, qui rappelle aux utilisateurs de ne jamais authentifier des opérations dont ils ne sont pas à l'initiative ni communiquer leurs mots de passe et codes confidentiels à des tiers, même leur banquier. L'Observatoire s'associe également à la campagne du « Fraude Fight Club » spécialement destinée aux 18-35 ans sur les réseaux sociaux, aux côtés du groupement d'intérêt public action contre la cybermalveillance.

Selon Bruno Le Maire, ministre de l'Économie, des Finances et de la Souveraineté industrielle et numérique : « « *En trois ans, notre action a permis de réduire de 30% le taux de fraude au paiement*
par internet. Mais, face au développement de nouvelles techniques de fraudes au paiement, nous
voulons agir vite pour protéger les Français. C'est ce que nous faisons avec ce nouveau cadre associant
la Banque de France, les associations de consommateurs, les professionnels des paiementsmais aussi
les e-commerçants et les opérateurs de téléphonie et d'internet. Nous renforçons la lutte contre la
fraude et nous facilitons les démarches de remboursement, même lorsqu'une authentification forte a
été réalisée. Nous luttons ainsi contre les fraudeurs et défendons le pouvoir d'achat des Français ».

Selon François Villeroy de Galhau, Gouverneur de la Banque de France et Président de l'Observatoire, « Ces recommandations illustrent l'engagement de l'ensemble des membres de l'Observatoire à faire face à deux grandes nécessités: d'une part, intensifier collectivement nos actions de prévention et de lutte contre la fraude et d'autre part, apporter des réponses clarifiées et harmonisées aux victimes de fraude ».

PARIS – 16 MAI 2023