COUNTRY:France
PAGE(S) :49-50
SURFACE :167 %
FREQUENCY :Monthly
CIRCULATION :(9763)
AVE :9,18 K€
AUTHOR :Gilles Vaysset
► 1 March 2025 - N°902
Page Source

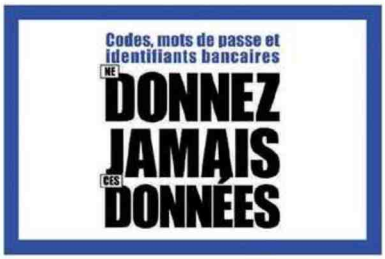
MÉDIATION

Fraude à la carte en ligne : l'authentification même forte n'exclut pas la vigilance

Les fraudes au paiement sont de plus en plus sophistiquées. Avec le développement de la fraude par manipulation, la double authentification n'est pas une barrière inviolable. Rappel des règles et des bonnes pratiques des banquiers et consommateurs.

Gilles Vaysset
Médiateur
ASF

Trop nombreuses sont les victimes de fraudes au paiement alors qu'elles croient parler à un conseiller bancaire. Ce fléau a une caractéristique : il touche tant les consommateurs que les établissements bancaires qui font face à l'insatisfaction de leur clientèle. Un coût aussi. En 2023, l'Observatoire de la sécurité des moyens de paiement a évalué la fraude au faux conseiller bancaire à 379 millions d'euros.



La campagne anti-fraude réalisée par la place.

Au 1er semestre 2024, cette fraude par manipulation a amorcé un repli. Pour autant, en 2024, 20 % des saisines traitées par le médiateur de l'Association française des sociétés financières ont concerné ce sujet (35 % en intégrant les cas de vols de cartes ou de fraudes aux virements).

Traitant les services de paiement dans le marché intérieur, la réglementation issue de la directive européenne DSP 2 du 25 novembre 2015 se veut pourtant très protectrice du consommateur. Elle met à la charge du banquier de recueillir le consentement du client à l'opération de paiement au moyen de procédés d'authentification renforcés, fondés sur deux critères relevant de la connaissance (par exemple un code), de la possession (un téléphone déclaré) ou de l'inhérence (reconnaissance digitale ou faciale). Dixit l'article L. 133-19 V du Code monétaire et financier : « *Sauf agissement frauduleux de sa part, le payeur ne supporte aucune conséquence financière si l'opération de paiement non autorisée a été effectuée sans que le prestataire de services de paiement du payeur n'exige une authentification forte du payeur prévue à l'article L. 133-44.* »

Un client négligent ?

Autre cas : l'opération a bien été authentifiée mais elle est considérée comme non autorisée par le client. L'établissement doit en plus prouver que ce dernier a fait preuve de négligence grave dans la conservation de ses données bancaires personnelles, voire qu'il est à l'origine de la fraude. En effet, l'article L. 133-19 IV du Code monétaire et financier énonce que « *le payeur supporte toutes les pertes occasionnées par des opérations de paiement non autorisées si ces pertes résultent d'un agissement frauduleux de sa part ou s'il n'a pas satisfait intentionnellement ou par négligence grave aux obligations mentionnées aux articles L. 133-16 et L. 133-17* », ces derniers articles traitant notamment de la nécessaire préservation par l'utilisateur de ses données de sécurité personnelles et confidentielles attachées à son instrument de paiement.

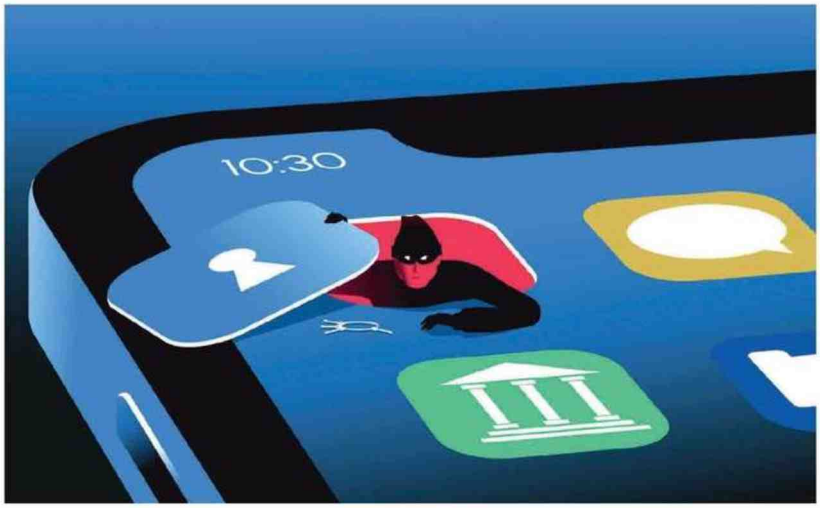
Un cas pratique, traité à la médiation de l'ASF, permet d'y voir plus clair. Madame N. a été victime d'une arnaque « assurance maladie » et a porté une réclamation auprès d'un établissement, qui a refusé de la rembourser de la somme de 3 500 euros frauduleusement débitée de son compte. La clientèle affirmait avoir répondu à un mail l'invitant à régler la somme de 1,20 euro pour mettre à jour sa carte Vitale. Après avoir effectué ce paiement, elle a été contactée par téléphone par une personne se présentant comme un salarié de l'établissement bancaire et a par la suite constaté un débit de 3 500 euros sur son compte. Opération immédiatement contestée !

Pour refuser de prendre en charge l'opération litigieuse, l'établissement a fait valoir d'une part que l'opération était correctement authentifiée, et d'autre part, que Madame N avait été gravement négligente. L'instruction de la saisine de Madame N nous a conduits à vérifier ces deux arguments.

Pas de quartier en cas d'absence d'authentification forte

Première étape : comme à chaque dossier de fraude que nous sommes amenés à traiter, nous avons demandé à

COUNTRY:France
PAGE(S) :49-50
SURFACE :167 %
FREQUENCY :Monthly
CIRCULATION :(9763)
AVE :9,18 K€
AUTHOR :Gilles Vaysset
► 1 March 2025 - N°902



l'établissement de nous transmettre le justificatif de l'authentification forte de l'opération. Nous avons alors pu constater que pour valider l'opération de paiement, il convenait de communiquer un code secret connu par le client seul (critère de connaissance) à partir du téléphone portable appartenant au client et déclaré à l'établissement (critère de possession). Cette procédure étant conforme aux exigences de la DSP2, nous avons considéré que l'opération avait été correctement authentifiée. À défaut, nous aurions par principe invité la banque à rembourser la totalité des sommes en cause.

Concernant la preuve de la négligence, l'objet du mail qu'elle avait reçu reflétait à lui seul son caractère manifestement frauduleux. En effet, ce message consistait à demander le règlement de la somme de 1,20 euro pour mettre à jour une carte Vitale. Or, celle-ci est gratuite, ce qui aurait dû alerter Madame N et l'inciter à la prudence. Par ce faux lien, l'escroc a pu enregistrer les coordonnées de sa carte et des informations complémentaires personnelles (adresse, numéro de téléphone…), lui permettant de mettre Madame N en confiance par la suite. Nous avons aussi relevé que Madame N précisait dans son dépôt de plainte avoir conversé avec l'escroc au téléphone, entretien au cours duquel le paiement a été authentifié. Nous avons noté qu'elle avait été contactée depuis un numéro de type 07.44.xx.xx.xx dont le format ne correspondait pas à celui des numéros de téléphone de sa banque, ni d'aucune puisque ces dernières n'appellent pas à partir de mobiles, ce qui aurait également dû attirer son attention.

Besoin de clarté dans le message

Nous avons enfin vérifié le message qu'elle a reçu de son prestataire de services de paiement et qui accompagnait l'authentification. En effet, pour valider le paiement, Madame N a reçu une notification sur son application mobile avec les détails de l'opération à valider : type d'opération, montant, date, heure et commerçant. Le téléphone de Madame N étant un critère retenu par l'établissement pour authentifier le paiement, et ce dernier n'ayant pas été déclaré ni volé, ni perdu, il était donc établi que celle-ci avait validé l'opération malgré l'ensemble des informations fournies. Au total, nous avons considéré que ces agissements étaient de nature à caractériser une négligence grave de sa part au sens jurisprudentiel du terme, ayant permis la réalisation de l'opération litigieuse. En conséquence, nous avons estimé que l'établissement n'était en effet pas tenu de prendre en charge le montant de l'opération frauduleuse.

Ce procédé très fréquent est parfois décliné. Tout part d'un faux message de la Sécurité Sociale, des impôts, d'un service de colis, qui permet, sous prétexte d'un renouvellement, d'une actualisation ou d'un nouveau rendez-vous moyennant une modique somme de l'ordre de l'euro, de récupérer les coordonnées de la carte bancaire, puis à appeler en se faisant passer pour un conseiller de la banque afin de finaliser une opération de paiement que l'escroc a initiée, avec des prétextes divers dont le plus fréquent consiste à procéder à l'annulation de l'opération qui va précisément être validée !

Besoin d'information, encore et toujours

Deux enseignements principaux semblent pouvoir être tirés :

– les prestataires de services de paiement mettent de plus en plus explicitement en garde leurs clients dans leurs messages. À cet égard, il convient de rappeler la recommandation numéro 11 de l'Observatoire de la sécurité des moyens de paiement portant sur la nécessité d'informer l'utilisateur à chaque étape du processus d'authentification, en délivrant au consommateur une information explicite concernant la nature de l'opération en cours, et éviter les messages trop succincts du type « pour valider l'opération » qui, sans mentionner qu'il s'agit d'une opération de paiement, le montant et le bénéficiaire, facilitent de ce fait la fraude ;

– au-delà des avertissements au moment de la validation des paiements, il est encore durablement nécessaire de mieux informer les consommateurs sur les risques qu'ils encourent en général et de compléter utilement leur éducation économique et financière. On peut cependant redouter que les médiateurs restent longtemps saisis de cas de fraude. Le diable se cache dans les détails, comme l'on sait, et le fraudeur s'efforce de trouver les failles résultant de certains choix techniques concernant les critères d'authentification ou des possibilités d'exemption que les règlements prévoient dans certains cas. Néanmoins, l'étau se resserre. D'où la nécessité de ne pas relâcher les efforts de sensibilisation. ■