

MÉDIATION

Quand la fraude au paiement passe par le RIO...



Gilles Vayssat

Médiateur de l'ASF

Savez-vous que, pour changer d'opérateur téléphonique, il faut impérativement une donnée : le relevé d'identité opérateur ou RIO ? Les fraudeurs, eux, le savent, prompts à s'approprier cet élément pour se livrer à leur besogne. Au vu du droit et de l'équité, ce sujet mérite d'être creusé s'il prend de l'ampleur. Avis aux clients, aux banquiers et aux opérateurs de téléphonie.

On le sait, l'imagination des fraudeurs est fertile. La lutte contre le fléau des arnaques au paiement est une suite de combats dans lesquels la technique tient bien sûr un rôle essentiel. Mais elle doit être relayée par une bonne information susceptible d'orienter le comportement des consommateurs vers de meilleures pratiques. Aussi, semble-t-il important d'évoquer une

s'obtient aisément en passant par un numéro d'appel commun à tous les opérateurs. Comment le fraudeur fait-il pour en disposer ? Par exemple, en se faisant passer pour un agent de l'opérateur téléphonique de son interlocuteur, pour les besoins d'une prétendue vérification, ou pour un agent de sa banque, au motif de confirmer le numéro de téléphone déclaré à la banque comme associé à son compte ou à sa carte.

RIO : le fraudeur prend le contrôle de votre ligne

Comment s'en sert-il ensuite ? Après avoir obtenu les données bancaires de sa victime, le plus souvent par phishing, le fraudeur bascule le numéro de téléphone sur son propre mobile grâce au RIO obtenu. Dès lors, il dispose d'une fenêtre de temps pour effectuer quelques paiements en totale discrétion puisque c'est lui qui récupère les codes d'authentification envoyés par SMS.

Entre l'obtention du RIO et la commission de la fraude, il peut se passer un certain temps. Toutefois, un jour, le consommateur constate que son téléphone ne fonctionne plus : il appelle alors son fournisseur qui lui

indique que sa ligne a été transférée à un autre opérateur. Il demande bien sûr un autre numéro, avant de s'apercevoir assez vite que son compte bancaire a été débité de plusieurs opérations qu'il n'a jamais passées. Il se retourne alors vers sa banque : elle lui répond que ces opérations ont bien été validées par ses soins. Il les conteste, mais la banque, forte d'une authentification conforme à la DSP2, considère qu'il est à l'origine de ces opérations ou qu'il a transmis des informations confidentielles à un tiers, et refuse de les prendre à sa charge.

Juridiquement : la victime est en tort

Compte tenu du dépôt de plainte qui fait le plus souvent suite à ce type de situations, il s'agit pour le médiateur d'opérations non autorisées. Concrètement, la victime n'a eu aucune conscience des opérations débitées de son compte, puisqu'elle n'a jamais reçu de SMS de la part de sa banque lui demandant de les valider et, partant, n'a jamais été sollicitée par quiconque pour donner les codes reçus. Les critères d'authentification sont certes remplis, mais par quelqu'un d'autre, qui reçoit au numéro de téléphone de sa victime les codes nécessaires à la validation des opérations.

Juridiquement, la victime a contrevenu à l'article L. 133-16 du Code monétaire et financier : « Dès qu'il reçoit un instrument de paiement, l'utilisateur de services de paiement prend toute mesure raisonnable pour préserver la sécurité de ses dispositifs de sécurité personnalisés. »

« Dans la mesure où le RIO constitue un des éléments de la sécurité des opérations de paiement, il doit faire l'objet des mêmes précautions que les autres éléments d'authentification. »

nouvelle forme de manipulation, ressemblant au SIM swapping. On voit apparaître cette manipulation dans les saisines du médiateur et elle susceptible de prendre de l'ampleur : elle consiste à obtenir d'un consommateur le RIO de son téléphone portable.

RIO, de quoi s'agit-il ? C'est le relevé d'identité opérateur, qui permet la portabilité du numéro de téléphone en cas de changement d'opérateur. Il



Dès lors que le numéro de téléphone constitue l'un des deux critères d'authentification exigés par la DSP2, il devient alors un élément concourant à la sécurité de ses paiements. Donner son RIO est ainsi constitutif d'une négligence grave. La banque n'est donc pas tenue, aux termes de l'article L. 133-19, de rembourser son client.

Pour autant, reconnaissons qu'il n'y a rien d'évident à identifier le code RIO comme une donnée sensible, partie intégrante du dispositif de sécurité de sa carte bancaire. Le numéro de la carte, son code, sa date de validité, son cryptogramme, en font partie, tout le monde le sait ou s'en doute. Mais le code RIO ? Qui plus est, il n'y a aucun espoir de pouvoir arrêter la fraude, par exemple en faisant opposition, puisque le consommateur est dans l'ignorance totale de ce qui se passe.

Un partage des responsabilités par mesure d'équité

Pour tenir compte de cette réalité, et en équité, j'ai proposé jusqu'à présent dans ces cas récents que la banque prenne en charge la moitié de la fraude. Cela me semble justifié par l'état de conscience ou d'insuffisante information du consommateur. Les consommateurs ne réalisent généralement pas, dans un premier temps, qu'ils ont été victimes d'une manœuvre frauduleuse. C'est ce que nous constatons en médiation.

En effet, les courriers accompagnant leur saisine sont souvent laconiques et se limitent à contester des débits apparus sur leur compte. Pourtant,

l'origine de ces opérations résulte fréquemment d'une première attaque de type phishing, par l'envoi d'un courriel frauduleux redirigeant le client vers un site internet contrefait, reproduisant fidèlement le site officiel de leur établissement bancaire ou un site d'achat, sur lequel il renseigne ses données bancaires confidentielles qui sont interceptées par le fraudeur. Mais le mal n'intervient qu'ensuite, plus ou moins longtemps après. Munis des identifiants de connexion à l'espace client et à l'aide du code RIO recueilli dans un deuxième temps, les fraudeurs agissent ensuite de façon totalement autonome et peuvent procéder à diverses opérations d'achat sans que leur victime en ait immédiatement connaissance.

Les opérateurs de téléphonie ont leur rôle à jouer

La banque n'ayant pas été informée, au moment où le fraudeur agit, du changement de numéro de téléphone de son client, elle n'a pas de raison de bloquer les paiements contestés. La fraude cesse bien sûr dès que ce dernier a averti la banque de son changement de ligne téléphonique, ce qu'il lui incombe de faire avec diligence, sous peine de négligence grave. Pour améliorer l'état d'information des consommateurs, communiquer préventivement et influencer positivement sur leur comportement, il conviendrait qu'une demande de RIO ou un changement d'opérateur avec transfert de lignes s'accompagne systématiquement de messages de précaution – ce qui

n'est pas toujours le cas –, voire d'un processus d'authentification au moment du basculement de la ligne. Dans la mesure où le RIO constitue, selon les choix de sécurité effectués par le prestataire de services de paiement, un des éléments de la sécurité des opérations de paiement, il doit faire l'objet des mêmes précautions que les autres éléments d'authentification. Sur ce point, et surtout si ce type de fraude est appelé à grossir, les banques ne peuvent être laissées seules face aux victimes : les opérateurs de téléphonie devraient remplir un rôle pour aider à sécuriser les comptes de ceux qui sont aussi leurs clients. ■

Tous les mois, un sujet sur la « Médiation » dans *Revue Banque*

Retrouvez les articles de :

Arnaud Chneiweiss,
médiateur de l'assurance



Marielle Cohen-Branché,
médiateur de l'Autorité
des marchés financiers



Gilles Vaysset, médiateur
de l'ASF

