Instruments de paiement et de crédit

Leçon 1004 : La carte de paiement : cas pratique

Marie-Andrée RAKOTOVAHINY

Table des matières

Enoncé des faits :

Hier, Pauline a fait opposition à sa carte bancaire en raison de deux débits frauduleux opérés sur le site internet de deux magasins. Elle a passé ses achats après avoir répondu à un mail douteux de son opérateur de fourniture internet lui permettant de payer sa facture téléphonique. Au moment de ces transactions, sa carte était en sa possession et sous son contrôle. Elle sollicite le remboursement de ces transactions par sa banque qui lui oppose un refus. La banque motive son refus par le fait qu'elle ne s'est pas assez renseignée sur son opérateur internet alors que le mail lui semblait douteux, et qu'elle n'a pas vérifier que le prélèvement automatique mis en place n'avait pas fonctionné. La banque est-elle fondée à refuser le remboursement ?

En savoir plus : Corrigé

Pauline a été victime de *phishing*. En matière de *phishing*, la jurisprudence essaie de trouver un équilibre entre l'affichage d'une solution favorable pour l'utilisateur et une solution de sévérité à l'égard du prestataire de service de paiement. Dans notre affaire semble t-il Pauline a fait preuve d'une négligence en répondant à un mail qu'elle présumait douteux et dans lequel elle a fournit sans doute des données personnelles et confidentielles. Le traitement de cette affaire dépendra de l'appréciation des juges du fond.

Exemples jurisprudentiels :

- Cass. com., 18 janv. 2017, n° 15-18102 : « *Mais attendu que si, aux termes des articles L. 133-16 et L. 133-17 du code monétaire et financier, il appartient à l'utilisateur de services de paiement de prendre toute mesure raisonnable pour préserver la sécurité de ses dispositifs de sécurité personnalisés et d'informer sans tarder son prestataire de tels services de toute utilisation non autorisée de l'instrument de paiement ou des données qui lui sont liées, c'est à ce prestataire qu'il incombe, par application des articles L. 133-19, IV, et L. 133-23 du même code, de rapporter la preuve que l'utilisateur, qui nie avoir autorisé une opération de paiement, a agi frauduleusement ou n'a pas satisfait intentionnellement ou par négligence grave à ses obligations ; que cette preuve ne peut se déduire du seul fait que l'instrument de paiement ou les données personnelles qui lui sont liées ont été effectivement utilisés ; qu'ayant souverainement retenu qu'il ne résultait pas des pièces versées aux débats la preuve que M. X... avait divulgué à un tiers, de manière intentionnelle, par imprudence ou par négligence grave, des éléments d'identification strictement confidentiels ayant permis les paiements contestés et que la Caisse se bornait à évoquer l'hypothèse d'un « hameçonnage », en prétendant que M. X... avait certainement répondu à un courriel frauduleux qu'il pensait émaner de la Caisse pour qu'il renseigne un certain nombre de points dont les identifiants, mots de passe et codes de clefs qui permettent de réaliser les opérations à distance, sans en apporter la démonstration, c'est exactement que la juridiction de proximité, qui n'était pas tenue de suivre les parties dans le détail de leur argumentation et a procédé à la recherche prétendument omise, a accueilli la demande de remboursement de M. X...* ».
- Cass. com., 25 oct. 2017, n° 16-11644, « *Qu'en se déterminant ainsi, sans rechercher, au regard des circonstances de l'espèce, si Mme Y... n'aurait pas pu avoir conscience que le courriel qu'elle avait reçu était frauduleux et si, en conséquence, le fait d'avoir communiqué son nom, son numéro de carte bancaire, la date d'expiration de celle-ci et le cryptogramme figurant au verso de la carte, ainsi que des informations relatives à son compte SFR permettant à un tiers de prendre connaissance du code 3D Secure ne caractérisait pas un manquement, par négligence grave, à ses obligations mentionnées à l'article L. 133-16 du code monétaire et financier, la juridiction de proximité a privé sa décision de base légale* ».
- Cass. com., 28 mars 2018, n° 16-20018, « *Vu les articles L. 133-16 et L. 133-19 du code monétaire et financier ; Attendu que pour statuer comme il fait, l'arrêt, après avoir relevé que M. Y... a été victime d'un hameçonnage, ayant reçu des courriels successifs portant le logo parfaitement imité du Crédit mutuel accompagnés d'un "certificat de sécurité à remplir attentivement" qu'il a scrupuleusement renseignés, allant même jusqu'à demander à la banque la communication de sa nouvelle carte de clefs personnelle pour pouvoir renseigner complètement le certificat litigieux, ce qui montre sa totale naïveté, retient que la banque convient que seul un examen vigilant des adresses internet changeantes du correspondant ou certains indices, comme les fautes d'orthographe du message, sont de nature à interpeller le client, ce à quoi n'est pas nécessairement sensible un client non avisé, étant observé que M. Y..., qui ne se connectait quasiment jamais au site internet de la banque, ignorait les alertes de cette dernière sur*

le hameçonnage, puis en déduit que c'est à son insu que M. Y... a fourni les renseignements qui ont permis les opérations frauduleuses sur son compte et que n'est pas constitutive d'une négligence grave le fait pour un client "normalement" attentif de n'avoir pas perçu les indices propres à faire douter de la provenance des messages reçus ; Qu'en statuant ainsi, alors que manque, par négligence grave, à son obligation de prendre toute mesure raisonnable pour préserver la sécurité de ses dispositifs de sécurité personnalisés l'utilisateur d'un service de paiement qui communique les données personnelles de ce dispositif de sécurité en réponse à un courriel qui contient des indices permettant à un utilisateur normalement attentif de douter de sa provenance, peu important qu'il soit, ou non, avisé des risques d'hameçonnage, la cour d'appel a violé les textes susvisés ».