Phishing, paiements frauduleux et responsabilité de la banque

Commentaire d'arrêt publié le **25/09/2020**, vu **828 fois**, Auteur : Laurent LATAPIE Avocat

La victime d'un phishing sur son compte bancaire faisant l'objet de prélèvements frauduleux demeure t'elle démunie ou peut-elle se retourner contre sa banque pour engager sa responsabilité?

Il convient de s'intéresser à un arrêt de la Cour de Cassation qui a été rendu en juillet dernier et qui vient aborder la problématique de la responsabilité de l'établissement bancaire lorsque ce dernier fait passer des opérations de paiement non autorisées.

Cette jurisprudence est intéressante en ce qu'elle rappelle qu'il résulte de l'article L. 133-19, IV, du Code Monétaire et Financier, que le payeur supporte toutes les pertes occasionnées par des opérations de paiement non autorisées s'il n'a pas satisfait par négligence grave, exclusive de toute appréciation de sa bonne foi, à l'obligation, imposée à l'utilisateur de services de paiement par l'article L. 133-16 du même code, de prendre toute mesure raisonnable pour préserver la sécurité du dispositif de sécurité personnalisé mis à sa disposition.

Dans cette affaire Monsieur V., titulaire d'un compte ouvert au sein d'un établissement bancaire a, en novembre 2015, contesté des opérations de paiement effectuées, selon lui frauduleusement, sur son compte et a demandé à la banque de lui en rembourser le montant.

Se heurtant au refus de celle-ci, qui lui reprochait d'avoir commis une faute en donnant à un tiers des informations confidentielles permettant d'effectuer les opérations contestées, Monsieur V a assigné la banque en remboursement des sommes débitées sur son compte et en paiement de dommages-intérêts.

Or, Monsieur V avait été victime d'un phishing et d'un prélèvement frauduleux qui avait été réalisé sur son compte bancaire.

Il convient de rappeler 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 L133.19, IV et L133.23 du même Code, de rapporter la preuve que l'utilisateur, qui nie n'avoir pas satisfait, par négligence grave, à ses obligations, a réellement commis une telle négligence.

Or la banque confond bien souvent démonstration et présomption en se retranchant bien souvent derrière l'imprudence de son client.

En l'espèce, Monsieur V avait reçu le 24 novembre 2015 à 1h39 un e-mail non personnalisé, dont le texte avait une syntaxe approximative et dont le contenu était sans lien avec la réalité du sociétaire, car, à aucun moment, ce dernier n'avait été informé de l'existence d'une nouvelle réglementation concernant la fiabilité des achats par carte bancaire.

Il est vrai que Monsieur V avait commis une négligence grave en cliquant sur le lien proposé.

Cependant, Monsieur V était un client de bonne foi qui avait été la victime d'une fraude commise à son encontre par un tiers, de sorte qu'il n'était pas totalement responsable de son préjudice.

C’est alors au payeur de supporter l'intégralité des pertes occasionnées par des opérations de paiement non-autorisées dès lors que 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 du Code Monétaire et Financier.

Dès lors, la Cour de Cassation considère que manque, par négligence grave, à son obligation de prendre toute mesure raisonnable pour préserver la sécurité de ses dispositifs de sécurité personnalisés de telle sorte que pour la banque, 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, de bonne foi engage sa responsabilité et exonère celle de la banque.

Celle-ci considérait qu’elle ne pouvait être condamnée à prendre en charge tout ou partie d'un paiement effectué à partir du compte de son client que s'il a commis une faute en effectuant ledit paiement et que ces opérations n'avaient pu être réalisées qu'à raison de la négligence grave de ce dernier qui avait répondu à un courriel d'hameçonnage.

Pour autant il y a lieu de constater que Monsieur V avait reçu le 24 novembre 2015 à 1h39 un e-mail non personnalisé, dont le texte avait une syntaxe approximative et dont le contenu était sans lien avec la réalité du sociétaire, car, à aucun moment, ce dernier n'avait été informé de l'existence d'une nouvelle réglementation concernant la fiabilité des achats par carte bancaire.

La banque en a déduit que Monsieur V a donc commis une négligence grave en cliquant sur le lien proposé.

Fort heureusement la Cour de Cassation ne partage pas cette analyse et vient rappeler que la banque engage malgré tout sa responsabilité.

Elle considère que le juge du fond doit vérifier si Monsieur V avait commis une négligence grave en répondant à un courriel présentant de sérieuses anomalies tenant tant à la forme qu'au contenu du message qu'il comportait pour déterminer s’il engageait sa responsabilité.

Article rédigé par Maître Laurent LATAPIE,

Avocat, Docteur en Droit,

www.laurent-latapie-avocat.fr