UTILISATION FRAUDULEUSE DE LA CARTE BANCAIRE

La crise de la COVID 19 a entrainé une hausse significative de l'utilisation de la carte bancaire, notamment avec l'option « sans-contact ». Cependant, l'utilisation frauduleuse de ce moyen de paiement s'est également renforcée.

La fraude à la carte bancaire peut se réaliser par divers moyens et techniques. Ainsi, même dans l'hypothèse où vous êtes encore en possession de votre carte bancaire, vous pouvez être victime d'une utilisation frauduleuse de celle-ci. Il convient donc de vérifier régulièrement les opérations réalisées sur votre compte bancaire.

Que faire en cas d'utilisation frauduleuse de votre carte bancaire ?

Dès que vous avez connaissance d'une ou plusieurs opérations frauduleuses, il convient de faire opposition au moyen de paiement dans les meilleurs délais.

Néanmoins, si vous n'avez pas constaté rapidement les opérations frauduleuses, vous disposez de **13 mois** pour informer votre établissement bancaire et faire opposition au titre de l'*article L. 133-24 du Code monétaire et financier* (alinéa 1er *« l'utilisateur de services de paiement signale**, sans tarder**, à son prestataire de services de paiement une opération de paiement non autorisée ou mal exécutée et **au plus tard dans les treize mois suivant la date de débit** sous peine de forclusion à moins que le prestataire de services de paiement ne lui ait pas fourni ou n'ait pas mis à sa disposition les informations relatives à cette opération de paiement (…)* »).

Cependant, lorsqu'une opération frauduleuse est réalisée en dehors de l'espace économique Européen, le délai passe alors à 70 jours (sauf délai contractuel plus long inséré dans votre Convention de compte, délai ne pouvant excéder 120 jours).

Pour ce faire, votre établissement bancaire doit mettre à votre disposition des moyens appropriés, vous permettant de réaliser votre opposition et doit également vous fournir une preuve de la bonne réception de votre opposition (article L133-15 du Code monétaire et financier).

Vous pouvez également déposer plainte auprès des services de police, de gendarmerie ou directement auprès du Procureur de la République. Les services de police et de gendarmerie ont l'obligation de recevoir votre plainte (article 15-3 du Code de Procédure pénale).

Quelles sont les obligations de votre établissement bancaire ?

Elles varient en fonction de l'utilisation frauduleuse de votre carte.

Au titre de l'article. L. 133-18 du Code monétaire et financier, votre établissement bancaire est dans l'obligation de procéder au remboursement des opérations frauduleuses immédiatement ou au plus tard à la fin du premier jour ouvrable suivant.

Votre banque doit ainsi rétablir votre compte dans l'état où il se serait trouvé si l'opération frauduleuse n'avait pas eu lieu. Elle est donc tenue de procéder au remboursement des frais de découvert ou d'incidents de paiement.

Néanmoins, il est à noter que lorsque vous n'êtes plus en possession de votre moyen de paiement (suite à la perte ou au vol de votre carte), les sommes frauduleusement prélevées avant votre opposition peuvent ne pas vous être remboursées en totalité.

En effet, au titre de l'article L.133-19 du Code monétaire et financier « *En cas d'opération de paiement non autorisée consécutive à la perte ou au vol de l'instrument de paiement, le payeur supporte, avant l'information prévue à l'article L. 133-17 [l'opposition], les pertes liées à l'utilisation de cet instrument, dans la limite d'un plafond de 50 euros* ».

Votre banque peut donc déduire la somme de 50 € au montant rétrocédé. Cependant, cette retenue n'a pas à être pratiquée si l'opération de paiement non autorisée a été effectuée sans utilisation du code de sécurité.

Votre établissement bancaire peut-il refuser de procéder au remboursement des opérations frauduleuses ?

Il peut effectivement refuser de procéder au remboursement dans l'hypothèse où il soupçonne une fraude ou une négligence grave de votre part. En effet, en tant que titulaire de votre carte bancaire, vous devez prendre « *toute mesure raisonnable pour préserver la sécurité de [vos] données de sécurité personnalisées* ».

Il appartient alors aux juges, *in fine*, de déterminer si votre comportement correspond à une négligence suffisamment grave. Les juges ont ainsi pu retenir que le fait d'annoter le code confidentiel sur sa carte bancaire s'analyse en un comportement négligeant, permettant à la banque de ne pas procéder au remboursement des sommes frauduleusement dérobées.

A cet égard, une nouvelle question a été soulevée concernant la pratique du « phishing » ou de l'hameçonnage, qui consiste à obtenir via un courriel, un SMS ou un appel frauduleux les informations confidentielles permettant ainsi au fraudeur de réaliser un paiement (notamment votre numéro de carte bancaire, le code confidentiel de votre carte, etc.). Les fraudeurs peuvent utiliser de fausses identités, vous induisant en erreur afin de soutirer les informations nécessaires à leurs méfaits. Vous fournissez alors volontairement des informations confidentielles aux fraudeurs.

Or, les juges ont pu adopter une position très sévère à l'égard des victimes de hameçonnage en considérant que la délivrance d'informations confidentielles est une grave négligence de la part du

titulaire de la carte et que ce de fait, la banque n'était pas dans l'obligation de rembourser la victime (pour exemple : Cour de cassation, civile, Chambre commerciale, 1 juillet 2020, 18-21.487, la Cour de cassation a ici estimé que dans la mesure où le courriel auquel avait répondu la victime de hameçonnage comportait de sérieuses anomalies, son comportement devait être analysé comme négligeant).

Néanmoins, la Cour de Cassation, dans un *arrêt du 23 novembre 2019,* a pu indiquer que « il *ne résulte d'aucune constatation de l'arrêt que le message d'hameçonnage…en réponse auquel, à supposer ce fait établi, Mme L. aurait communiqué des données personnelles liées à son instrument de paiement, ait contenu des indices permettant à un utilisateur normalement attentif de douter de sa provenance* ».

Aussi, dans l'hypothèse où le courriel d'hameçonnage ne laisserait pas apparaitre d'éléments permettant à une personne normalement attentive de détecter la fraude, pourrait permettre à la victime d'obtenir une indemnisation.

Par ailleurs, il est important de noter qu'il appartient à l'établissement bancaire d'apporter la preuve de la négligence de son client. En effet, si votre banque est dans l'impossibilité de démontrer que vous avez été victime d'hameçonnage, elle ne pourra pas vous refuser le remboursement des sommes détournées.

Il est donc essentiel de ne pas divulguer d'information confidentielle et de rester toujours vigilent lorsque l'on vous demande ce type d'information. En effet, aucune administration ou société ne doit vous réclamer ce type d'information. En cas de doute, ne fournissez pas les informations réclamées et contactez par vous-même l'administration ou l'établissement afin de vérifier la véracité des propos. Les escrocs sont en effet très persuasifs et utilisent des procédés de plus en plus perfectionnés pour soutirer vos informations confidentielles.

Gaëlle SCHAEFFER

*article L133-18 du Code monétaire et financier : « *En cas d'opération de paiement non autorisée signalée par l'utilisateur dans les conditions prévues à l'article L. 133-24, le prestataire de services de paiement du payeur* ***rembourse au payeur le montant de l'opération non autorisée immédiatement après avoir pris connaissance de l'opération ou après en avoir été informé, et en tout état de cause au plus tard à la fin du premier jour ouvrable suivant****, sauf s'il a de bonnes raisons de soupçonner une fraude de l'utilisateur du service de paiement et s'il communique ces raisons par écrit à la Banque de France.* ***Le cas échéant, le prestataire de services de paiement du payeur rétablit le compte débité dans l'état où il se serait trouvé si l'opération de paiement non autorisée n'avait pas eu lieu*** ».