Utilisation frauduleuse de votre carte bancaire et responsabilité de la banque en cas d'hameçonnage,

Commentaire d'arrêt publié le **26/02/2023**, vu **1752 fois**, Auteur : Laurent LATAPIE Avocat

Quelle responsabilité de la banque en cas d'hameçonnage ou d'utilisation frauduleuse d'une carte bancaire bénéficiant d'un système d'authentification à distance 3D SECURE ?

Il convient de s'intéresser au cas, malheureusement trop fréquent en ces derniers temps, de l'utilisation frauduleuse de carte bleue par une tierce personne qui n'est pas le titulaire, et qui se retrouve en difficulté suite à ces mêmes prélèvements frauduleux mis en débit sur son compte bancaire.

Dans pareil cas, le premier reflexe du titulaire du compte, en sus de la plainte qu'il doit déposer, est de saisir sa banque pour qu'elle le rembourse.

Qui est responsable en cas d'utilisation frauduleuse de la carte bancaire ?

La question est alors posée de la responsabilité de la banque quant à la sécurisation de ce compte bancaire afin que l'établissement bancaire puisse garantir et rembourser le consommateur et client des opérations litigieuses qui ont été faites suite à l'utilisation frauduleuse de sa carte bleue par une tierce personne.

Or, en pratique, force est de constater que, trop souvent, ledit établissement bancaire refuse à son client la prise en charge des opérations litigieuses, laissant le client seul face à lui-même avec comme principale obligation de renflouer le compte bancaire des opérations litigieuses en question.

Pour autant, cette pratique de la banque n'est pas conforme à la jurisprudence rendue en la matière et qui vient pourtant consacrer la responsabilité de la banque en cas d'utilisation frauduleuse de la carte bleue d'un titulaire de compte.

En effet, il convient de rappeler que les établissements bancaires délivrent à leurs clients des moyens de paiement dont la carte bancaire fait partie.

Comment contester une opération bancaire frauduleuse ?

Les données entourant la carte bancaire, à savoir numéro de carte, pictogramme, code secret doivent être captés à l'aide de logiciels anonyme par des hackers qui revendent ces données et font du business de receleur en faisant ainsi une utilisation frauduleuse et malhonnête au détriment des victimes.

Cette problématique est malheureusement difficile à cibler car les hackers ou receleurs ont pour habitude de réaliser des retraits de petites sommes afin de rester naturellement discrets et ce, le plus longtemps possible.

Dès lors, il n'est pas rare de constater que plusieurs mois s'écoulent avant que le client, et titulaire du compte, se rende compte de la supercherie et de cette fraude bancaire lorsqu'il se rend compte finalement des opérations litigieuses qu'il n'a pas souhaitées, ni ordonnées, sont prélevées sur son compte bancaire.

Comment annuler une opération litigieuse ?

La victime contacte alors son établissement bancaire pour faire opposition à la carte bancaire utilisée frauduleusement et on ne peut que l'inviter à déposer plainte auprès des services compétents.

Il convient de rappeler que dans ces conditions, et ce, sans délai, l'établissement bancaire a l'obligation légale de rembourser le titulaire du compte avec le montant de la ou les sommes détournées frauduleusement, qu'il y ait eu ou non utilisation du code secret par une tierce personne et que le client soit resté ou non en possession de la carte bancaire en question.

Cela est expressément envisagé au travers de l'article L.133-18 du Code Monétaire et Financier qui indique qu'en cas d'opération de paiement non autorisée signalé par l'utilisateur, le prestataire de service de paiement du payeur, donc la banque, est tenu de rembourser au payeur le montant de l'opération non autorisée le cas échéant, en rétablissant le compte débité dans l'état où il se serait trouvé si l'opération de paiement litigieuse non autorisée n'avait pas eu lieu.

L'article L.133-20 du même Code précise encore qu'après avoir informé son prestataire aux fins de blocage du compte et d'un instrument de paiement, le payeur n'a pas vocation à supporter quelque conséquence financière que ce soit résultant de l'utilisation de cet instrument de paiement ou de l'utilisation détournée des données qui lui sont liées, sauf à ce que la banque rapporte la preuve d'un agissement frauduleux de sa propre part, ce qui n'est classiquement pas démontré mais parfois et malheureusement cela est plus que critiquable, bien souvent présumé ou subodoré par l'établissement bancaire qui ne trouve que cela à mettre en avant pour échapper à sa propre responsabilité.

Fort heureusement, plusieurs jurisprudences sont venues consacrer ce principe afin de ne pas mettre l'utilisateur et le consommateur en difficulté.

Il convient d'abord de citer la jurisprudence de la Cour d'Appel de PARIS, 8 septembre 2022, n°20-08102.

Quels sont les faits ?

Madame H. était titulaire d'un compte courant ouvert dans un établissement bancaire avec une carte bancaire associée.

Elle bénéficiait également d'un système d'authentification à distance dit « 3D SECURE » lui permettant d'effectuer des paiements à distance par internet saisissant un code à usage unique reçu par SMS avant de valider un paiement.

Divers paiements en ligne sont intervenus au profit de différentes enseignes commerciales connues et, affirmant avoir été victime d'opérations frauduleuses sur son compte et d'un détournement de sa carte bleue, Madame H. a saisi, le 19 février 2019, le Tribunal Judiciaire de PARIS d'une demande tendant principalement à la condamnation de la banque au remboursement des sommes en litige, soit la somme de 1.489,15 € outre de légitimes dommages

et intérêts.

Madame H. soutenait au visa des articles L.133-18, L.133-19 et L.133-20 du Code Monétaire et financier avoir été victime d'opérations frauduleuses sur son compte et d'un détournement de sa carte bancaire affirmant que le paiement en ligne avait été effectué à son insu.

Alors que les opérations litigieuses dataient du 21 juillet 2017 et du 21 octobre 2017, celle-ci avait avisé la banque de ces opérations le 9 novembre 2017 et avoir complété puis retourné le formulaire de contestation d'opérations par carte bancaire.

Madame H. rappelant que la banque avait finalement procédé à un remboursement seulement partiel sur son compte à hauteur de 1 221,52 €, laissant ainsi subsister un préjudice d'un montant de 1 489,15 €.

La preuve de la fraude ou de la négligence grave de l'utilisateur

Il convient de rappeler que l'article L.133-23 du Code Monétaire et Financier précise qu'il appartient au prestataire de service de paiement d'établir la preuve d'une fraude ou d'une négligence grave de l'utilisateur du service de paiement et non à l'utilisateur de prouver sa bonne foi et que rien ne permet d'attester que les transactions opérées sur son compte bancaire ont été dument validées par ses soins, ni que les SMS ont bien été envoyés et réceptionnés par cette dernière.

Pour autant, cela n'empêche pas la banque de tenter de s'exonérer de sa responsabilité en soutenant que les opérations litigieuses ont été validées par la saisie sur internet d'un code à usage unique envoyé par SMS sur le téléphone portable de Madame H., opérations qui n'avaient donc pu être autorisées que par cette dernière,

De telle sorte que les documents d'authentification ayant reçu le SMS contenant le code à usage unique correspondaient bien à celui de Madame H.,

Le code à usage unique authentifiant le paiement

A bien y croire la banque, Madame H. était bel et bien en possession de la carte bancaire associée à son compte lors des opérations litigieuses.

Dès lors, la banque considère que Madame H. est négligente et qu'elle a manqué à son obligation de surveillance de son compte, ce qui constitue la cause exclusive du préjudice dont la réalité reste à démontrer n'est que de son fait.

En effet, dans la mesure où les opérations litigieuses ont été validées par la saisie sur internet d'un code à usage unique envoyé par SMS sur son téléphone et donc autorisées par cette dernière, celle-ci ne pouvait raisonnablement évoquer l'utilisation frauduleuse de sa carte bleue.

Pour autant, la Cour d'appel de paris a une autre approche.

La Cour d'Appel de PARIS retient qu'il est constant que Madame H. est bien titulaire d'un compte courant ouvert dans les livres de l'établissement bancaire et associé à une carte bancaire, elle est bénéficiaire d'une authentification à distance dite « 3D SECURE » lui permettant d'effectuer des paiements à distance par internet en saisissant à usage unique reçu par SMS avant de valider un paiement.

Divers paiements en ligne sont intervenus pour un site d'enseigne connu.

Madame H. justifie avoir signalé à sa banque, dès le 9 novembre 2017, ne pas être à l'origine des ces paiements en niant avoir été destinataire des SMS, ce qu'elle a confirmé en complétant le

lendemain un formulaire de réclamation justifiant ainsi également avoir déposé une main courante le 14 novembre 2017.

La Cour souligne que pour rejeter la demande d'indemnisation de Madame H, le Premier Juge a considéré que la preuve était rapportée que la banque avait bien envoyé par SMS sur le numéro de téléphone de la requérante un code à usage unique permettant de valider l'opération et que la preuve d'une fraude n'était pas démontrée par Madame H. ni qu'elle se serait fait détourner sa carte bancaire à son insu.

Pour autant, la Cour d'Appel rappelle que si aux termes des articles L.133-16 et L.133-17 du Code Monétaire et Financier, il appartient à l'utilisateur de service de paiement de prendre toute mesure raisonnable pour préserver les dispositifs de sécurité personnalisés et d'informer sans tarder son prestataire de tel service de toute utilisation non autorisée de l'instrument de paiement ou des données qui lui sont liées, c'est à ce prestataire qu'il appartient en application des articles L.133-19 4 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.

Il est admis 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 entre les mains du client.

Ainsi, en cas d'utilisation d'un dispositif de paiement à sécurité personnalisée, il appartient également au prestataire, l'établissement bancaire, de prouver que l'opération en cause a été authentifiée, dument enregistrée et comptabilisée et qu'elle n'a pas été affectée par une déficience technique ou autre.

La preuve de l'authentification de l'opération litigieuse

En application des dispositions de l'article 9 du Code de Procédure Civile, il incombe à chaque partie de prouver les faits nécessaires au succès de sa prétention.

En l'espèce, la banque soutient que les codes ont bien été adressés à Madame H. et que par l'utilisation de ces codes à usage unique l'intéressée a valablement donnée son consentement pour réaliser les opérations de paiement en ligne litigieuses.

La banque soutient que le numéro de portable indiqué sur les documents d'authentification ait reçu les SMS contenant le code à usage unique correspond bien à celui de l'intéressée.

Pour autant, la seule pièce probante sur laquelle se fonde l'établissement bancaire est un relevé informatique retraçant deux opérations litigieuses, via le système 3D SECURE pour des sommes 407,17 € et 1 081,98 € indiquant l'envoi, pour chaque opération, d'un SMS au numéro de téléphone mobile appartenant à Madame H., numéro qu'elle ne conteste pas.

La Cour considère que ces éléments sont insuffisants à établir que Madame H. a bien été rendue destinataire de ces codes et à valablement donné son consentement aux opérations litigieuses et que le dispositif n'était pas affecté d'une déficience technique, ni encore que l'intéressée aurait contribué par sa faute ou par négligence à la réalisation desdites opérations,

D'autant plus que le fait de signaler la difficulté à sa banque le 9 novembre 2017 pour des paiements réalisés jusqu'au 21 octobre 2017 ne saurait être considéré comme tardif.

Il s’ensuit que c’est en inversant la charge de la preuve que le Premier Jugea débouté Madame H. de sa demande, de telle sorte que la banque sera tenue de payer et de rembourser Madame H. concernant les paiements litigieux.

Ainsi, la jurisprudence rappelle bien à travers une autre jurisprudence de la Cour d’Appel de RIOM, chambre commerciale, 14 septembre 2022, n°21/00236, qu’il incombe au prestataire de rapporter la preuve que l’utilisateur qui nie avoir autorisé une opération de paiement agit frauduleusement ou n’a pas satisfait intentionnellement ou par négligence grave à ses obligations, à la vigilance attendu d’un détenteur de la carte de paiement.

Au sens de la jurisprudence, cette vigilance doit être apprécié en tenant compte du fait que les internautes sont régulièrement destinataires de campagne d’information sur l’hameçonnage de la banque de la part des banques, des services publics et des associations de consommateurs.

Les campagnes d’information sur l’hameçonnage

Dès lors, peut constituer une négligence grave à son obligation de prendre toute mesure raisonnable pour préserver la sécurité de ces dispositifs de sécurité personnalisés le fait pour l’utilisateur d’un service de paiement de communiquer des données personnelles de ce dispositif en réponse à un courriel qui contient des indices permettant à un utilisateur normalement attentif de douter de sa provenance, peu important à cet égard que l’utilisateur ait agi de bonne foi.

Dès lors, cette jurisprudence est intéressante, étant d’ailleurs rappelé que la Cour de cassation a pris soin également de rappeler dans un jurisprudence récente du 30 novembre 2022, Cour de cassation, chambre commerciale, n°21-17.614, qu’il résulte des articles L.133-3 et L.133-6 du Code Monétaire et Financier qu’une opération de paiement initiée par le payeur qui donne un ordre de paiement à son prestataire de service de paiement est réputé autorisé uniquement si le payeur a également consenti au montant de l’opération.

L’utilisation frauduleuse de la carte bancaire

En vertu des articles L.133-18 et L.133-19 du Code Monétaire et Financier qu’en cas d’opération de paiement non-autorisé réalisé au moyen d'un instrument de paiement doté de données de sécurité personnalisées et signalées par l'utilisateur dans les conditions prévues par l'article L.133-24 du Code Monétaire et Financier, le prestataire de service de paiement du payeur rembourse au payeur le montant de l’opération non autorisée, sauf si la responsabilité du payeur est engagée en application de l’article L.133-19 du même Code.

Ainsi, en rejetant une demande de remboursement au motif que le fait qu’après que le titulaire d’une carte de paiement a introduit celle-ci dans un distributeur automatique de billets et a composé son code secret, un tiers compose à son insu le montant du retrait et s’empare des billets de banque ne constitue pas un cas d’exemption de la responsabilité du payeur prévue par l’article L.133-19 du Code Monétaire et Financier sans rechercher, ainsi que cela lui était demandé, si l’opération de paiement avait été autorisée en particulier quant à son montant et dans la négative sans constater que la responsabilité du payeur était engagée en application du 1 ou du 4 de l’article L.133-19 du Code Monétaire et Financier.

L’utilisation frauduleuse de la carte bancaire sur Internet

Il convient de saluer ces différentes jurisprudences qui viennent rappeler que, premièrement, au combien les hypothèses d'utilisations frauduleuses d'une carte bleue sur internet ou même au guichet sont nombreuses et fréquentes et, également, de rappeler que l'établissement bancaire engage sa responsabilité qui doit l'amener à rembourser le client titulaire du compte des opérations qu'il n'a pas validées.

Obligation pour laquelle, en pratique, force est de constater que la banque tente classiquement d'échapper à cette responsabilité et vient inverser la charge de la preuve en considérant que le titulaire du compte a été maladroit ou insuffisamment diligent quant à la sécurisation de ses propres données.

Toujours est-il que ces jurisprudences viennent rappeler qu'en cas d'opération de paiement non autorisée, le prestataire de service 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, en tout état de cause au plus tard à la fin du premier jour ouvrable suivant.

Il est donc important que l'établissement bancaire se le rappelle pour qu'il n'y ait aucune difficulté et que l'utilisateur qui a subi les opérations frauduleuses sur son compte soit finalement remboursé.

A défaut, il conviendra naturellement d'engager la responsabilité de la banque pour obtenir une condamnation judiciaire et le remboursement forcé des sommes frauduleusement prélevées sur le compte du titulaire.

A bon entendeur

Article rédigé par Maître Laurent LATAPIE,

Avocat à Fréjus, Avocat à Saint-Raphaël, Docteur en Droit,

www.laurent-latapie-avocat.fr