Quelle responsabilité de la banque en cas de « spoofing », lorsqu'un escroc se fait passer pour un conseiller de la banque ? Par Laurent Latapie, Avocat.

Parution : mercredi 2 juillet 2025

Adresse de l'article original :
https://www.village-justice.com/articles/quelle-responsabilite-banque-cas-spoofing-lorsqu-escroc-fait-passer-pour,53862.html

Le titulaire d'un compte bancaire se fait escroquer de plusieurs milliers d'euros par une personne se faisant passer pour un conseiller de la banque détenant des informations personnelles. Alerté par cette usurpation et ce « spoofing » la banque refuse de rembourser le client victime au motif qu'il aurait fait preuve d'une négligence grave. Que dis la jurisprudence ?

Il convient de s'intéresser à une jurisprudence qui a été rendue par la Cour de cassation, Chambre commerciale, ce 23 octobre 2024, N°23-16.277, et qui vient aborder la problématique de responsabilité de la banque lorsqu'un de ses clients, titulaire d'un compte, se fait escroquer par une tierce personne qui le contacte par téléphone et se fait passer pour un conseiller dudit établissement bancaire.

Quels sont les faits ?

Dans cette affaire, le 31 mai 2019, Monsieur J avait constaté que plusieurs virements frauduleux avaient été réalisés pour un montant de 54 500,00 € sur son compte ouvert dans les livres de la banque.

Monsieur J a alerté la banque le jour même, soutenant avoir été contacté par téléphone par une personne se faisant passer pour une préposée de l'établissement lui demandant d'ajouter, grâce à ses données personnelles de sécurité, cinq personnes sur la liste des bénéficiaires de virement.

Monsieur J a alors assigné la banque en remboursement de ces sommes.

La banque faisait griefs à la Cour d'appel de Versailles de l'avoir condamné à payer la somme de 54 500,00 € à Monsieur J avec intérêts au taux légal à compter du 10 octobre 2019 ainsi que la somme de 1 500,00 € à titre de dommages et intérêts pour préjudice moral avec intérêts au taux légal.

Pour la banque, celle-ci considérait que le payeur, à savoir le client titulaire du compte, supportait toutes les pertes occasionnées par les opérations de paiement non autorisé si ces pertes résultaient d'une négligence grave de sa part.

Le remboursement par la banque des opérations non autorisées sauf négligence grave.

Or, pour la banque, commet une négligence grave le payeur qui valide à distance et sans la vérifier une opération dont il n'est pas l'auteur.

Pour autant, la banque faisait grief à la Cour d'appel d'avoir relevé que, suivant ses déclarations, Monsieur J avait été contacté par téléphone par une personne se présentant comme assistante de sa conseillère bancaire qui lui avait expliqué qu'il avait été nécessaire de supprimer des bénéficiaires de virement pour déjouer une attaque informatique, qu'il fallait désormais les réenregistrer et qu'il était alors resté en ligne avec cette personne et avait reçu sur son téléphone mobile des messages l'invitant à valider des ajouts de bénéficiaires, ce qu'il avait fait en saisissant son compte confidentiel.

La banque faisait grief à la Cour d'appel d'avoir retenu que Monsieur J avait été gravement négligeant quand celui-ci avait validé les opérations dont il n'était pas l'auteur sans en vérifier toutes les données.

La banque rappelle encore que, selon elle, le payeur supporte toutes les pertes occasionnées par des opérations de paiement non autorisé si ces pertes résultent d'une négligence grave de sa part.

Négligence grave et faux conseiller bancaire.

Et, pour la banque, commet une négligence grave le payeur qui, à la demande d'une personne qui l'a contacté par téléphone en se présentant comme son conseiller bancaire valide à distance et sans la vérifier une opération dont il n'est pas l'auteur en dépit d'indices permettant l'utilisateur normalement attentif de douter de l'identité de son interlocuteur.

Or, en l'espèce, la Cour d'appel de Versailles avait relevé que, suivant ses déclarations, Monsieur J avait été contacté par téléphone par une personne se présentant comme une assistance de son conseiller bancaire qui lui avait expliqué qu'il avait été nécessaire de supprimer des bénéficiaires de virement pour déjouer une attaque informatique, qu'il fallait désormais les réenregistrer.

Qu'il était alors resté en ligne avec cette personne et avait reçu sur son téléphone mobile les messages l'invitant à valider des ajouts des bénéficiaires, ce qu'il avait fait en saisissant son compte personnel et qui lui avait enfin expliqué qu'il n'aurait plus accès à son compte et qu'il allait recevoir par la poste un nouvel identifiant de compte et un nouveau mot de passe.

La Cour d'appel retenait, quant à elle, que Monsieur J n'avait pas été gravement négligeant quand l'identité de son interlocutrice qui prétendait être non pas sa conseillère bancaire, mais l'assistante de celle-ci, l'objet de l'appel qui

tendait à réenregistrer des bénéficiaires de virement, ce qui pouvait pourtant se faire sans intervention d'un employé de la banque et ne présentait, au surplus, aucune urgence dans la mesure où Monsieur J n'aurait plus accès à son compte en ligne pendant plusieurs jours.

L'attaque informatique et la suppression de bénéficiaires de virement.

Et, les explications qui lui avaient été fournies suivant lesquelles l'attaque informatique dont il aurait été victime avait pu être déjouée par la suppression des bénéficiaires de virement qui lui fallait réenregistrer avant que l'accès en ligne à son compte soit bloqué et qu'un nouvel identifiant et un nouveau mot de passe lui soient adressés par voie postale, constituaient les indices permettant à un utilisateur normalement attentif de suspecter une fraude.

La banque allant même jusqu'à soutenir que, même de bonne foi, le payeur supporte toutes les pertes occasionnées par les opérations de paiement non-autorisées si ces pertes résultent d'une négligence grave de sa part.

Fort heureusement, la Cour de cassation ne partage pas cette approche-là.

En effet, elle précise dans cette jurisprudence qu'elle rejette le pourvoi de la banque en précisant qu'après avoir exactement énoncé qu'il incombe au prestataire de service de paiement de rapporter la preuve d'une négligence grave de son client, l'arrêt constate que le numéro d'appel apparaissait sur le numéro de portable de Monsieur J et s'était affiché comme étant celui de Madame Y, sa conseillère de la banque, et retient qu'il croyait être en relation avec une salariée de la banque lors du réenregistrement et de la nouvelle validation qu'elle sollicitait de bénéficiaires de virement sur son compte qu'il connaissait et qu'il a cru valider l'opération litigieuse sur son application dont la banque a assuré qu'il s'agissait d'une opération pour sécuriser.

Une vigilance diminuée par l'utilisation du "spoofing".

Il ajoute que le mode opératoire par l'utilisation du "spoofing" a mis Monsieur J en confiance et a diminué sa vigilance inférieure à un appel téléphonique émanant prétendument de sa banque pour lui faire croire au piratage de son compte à celle d'une personne réceptionnant un courrier, laquelle aurait pu disposer d'avantages de temps pour s'apercevoir d'éventuelles anomalies révélatrices de son origine frauduleuse.

De ses constatations et appréciations, la Cour d'appel a pu en déduire que la négligence grave de Monsieur J n'était pas caractérisée et c'est dans ces circonstances que la Cour de cassation rejette le pourvoi de l'établissement bancaire, ce qui vient confirmer l'indemnisation totale de Monsieur J, victime de ce "spoofing" et de cette escroquerie par téléphone.

Il convient quand même de rappeler que bon nombre de dispositions sont venues protéger le consommateur et une règlementation stricte est venue encadrer les opérations par carte, par virement et par prélèvement, notamment pour protéger au mieux le payeur.

Ainsi, des directives du Parlement Européen et de l'Union Européenne ont été mises en place le 13 novembre 2007 ainsi que le 25 novembre 2015.

Ces dispositions ont été transposées en droit Français.

Les dispositions protectrices du Code Monétaire et financier.

Ainsi, l'article L 133-24 du Code monétaire et financier prévoit dans son alinéa premier qu'en présence d'une telle opération non autorisée, il revient au payeur de le signaler à son prestataire de service de paiement.

Ce professionnel se verra alors dans l'obligation de rembourser le payeur conformément à l'article L 133-18 du Code monétaire et financier et ce, dans un bref délai, à charge pour l'établissement bancaire de rétablir ainsi le compte débité dans l'état où il se serait trouvé si l'opération non-autorisée n'avait pas eu lieu.

Une importante limite existe cependant en la matière puisque l'article L 133-19 4 du Code monétaire et financier précise qu'en matière d'opération de paiement par carte, par virement ou par prélèvement, le payeur supporte toutes les pertes occasionnées par des opérations de paiement non-autorisé si elles résultent des agissements frauduleux de sa part ou si ce même payeur 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.

L'obligation du titulaire du compte de préserver la sécurité de ses données bancaires.

Il convient de comprendre cette disposition comme l'obligation qui pèse sur le payeur de préserver la sécurité de ses données de sécurité personnalisée mais aussi d'en informer sans tarder son prestataire et son établissement bancaire de la perte, du vol, du détournement ou de toute utilisation non-autorisée de son instrument de paiement ou des données qui lui sont liées.

Or, la question qui se pose dans bon nombre de jurisprudences est de savoir comment comprendre la notion de négligence grave au sens de l'article L 133-19 4 du Code monétaire et financier.

Or, dans cette affaire, immanquablement Monsieur J avait été contacté par une personne qui, effectivement par ce biais de "spoofing", s'est fait passer par un conseiller bancaire mais sur la base d'informations confidentielles ou avec un numéro d'appel qui apparaissait sur le téléphone de Monsieur J s'affichant comme étant celui de sa conseillère.

La victime de "spoofing" non responsable d'une négligence grave.

De telle sorte que l'intéressé se croit être en relation avec une salariée de la banque lors du réenregistrement et de la nouvelle validation qu'elle sollicitait de bénéficiaires de virement, de telle sorte que cette personne, immanquablement

mal intentionnée, bénéficie d’informations confidentielles qui ne pouvaient qu’amener Monsieur J à être mis en confiance, voir en tout cas, diminuer sa vigilance.

De telle sorte que c’est donc à bon droit que la Cour de cassation, à la lueur des dispositions des articles L 133-24 et L 133-18 du Code monétaire et financier, a condamné la banque à rembourser Monsieur J des sommes qui ont été indûment perçues de son compte bancaire.

Laurent Latapie, Avocat à Fréjus et Saint-Raphaël, Docteur en Droit Barreau de Draguignan www.laurent-latapie-avocat.fr

L'auteur déclare ne pas avoir utilisé l'IA générative pour la rédaction de cet article.