L'utilisation frauduleuse d'un instrument de paiement et la négligence grave du titulaire du compte, qu'en est-il en matière de responsabilité ? Par Laurent Latapie, Avocat.

Parution : lundi 23 décembre 2024

Adresse de l'article original :
https://www.village-justice.com/articles/utilisation-frauduleuse-instrument-paiement-negligence-grave-titulaire-compte,51825.html

Si en droit bancaire, le titulaire d'un compte supporte toutes les pertes occasionnées par des opérations de paiement non autorisées si ces pertes résultent d'une négligence grave de sa part, qu'en est-il lorsque celui-ci a été victime d'un « *spoofing* » ou d'une usurpation d'identité d'un escroc, se faisant passer pour un conseiller bancaire, bénéficiant d'informations confidentielles et faisant valider des paiements par carte bleue qui se révèlent être finalement une arnaque ? La banque engage-t-elle sa responsabilité et doit-elle garantir la victime des sommes qui lui ont été retirées ?

Il est de ces jurisprudences qui sont attendues par les consommateurs parfois plus que d'autres.

J'en veux pour preuve notamment cette jurisprudence qui a été rendue par la Cour de cassation ce 23 octobre 2024, N° de pourvoi 23-16.267, et qui vient aborder la délicate problématique d'utilisation frauduleuse de carte bleue par des tierces personnes qui contactent par téléphone des clients en se faisant passer pour des responsables de la banque fort d'informations d'ailleurs très personnelles et confidentielles qui mettent en confiance.

L'escroquerie bancaire, nouveau fléau ?

Ledit client, mis en confiance, s'en remet à son interlocuteur pensant très honnêtement avoir affaire à un responsable ou un collaborateur de l'établissement bancaire et en lui donnant des informations qui vont finalement permettre à cette tierce personne, qui n'est finalement qu'un escroc, de prendre des centaines, voire, des milliers d'euros au détriment de ce client, lequel, bien souvent, se rend compte, d'ailleurs assez rapidement, mais trop tard, de la supercherie.

Malheureusement, cette technique d'escroquerie est en train de se développer de manière quasi hémorragique.

Dans pareil cas, très rapidement, le client prévient immédiatement l'établissement bancaire et vient solliciter sa banque au titre de ses différentes garanties pour que celle-ci vienne rembourser le client qui s'est fait malheureusement escroquer par des tierces personnes qui seront de toute façon à jamais introuvables et inidentifiables.

Le refus des banques de prendre en charge ses escroqueries.

Or, ces établissements bancaires, qui sont effectivement exposés à cette pratique qui se multiplie, ont comme premier réflexe finalement de refuser de prendre en charge le sinistre, de rembourser le client, et vient même, c'est un comble, finalement lui reprocher une négligence grave en acceptant de communiquer par téléphone des informations confidentielles, empêchant dès lors toute garantie de l'établissement bancaire.

Bon nombre de procès ont été enclenchés, et bon nombre de décisions de justice ont été rendus par les juges du fond, tantôt dans un sens, tantôt dans un autre,

Il était enfin temps que la Cour de cassation s'exprime sur le sujet.

C'est chose faite.

Ainsi, la Cour de cassation précise qu'aucune négligence grave au sens de l'article L133-19 du Code monétaire et financier ne peut être imputée au titulaire d'un compte qui est contacté téléphoniquement par une personne se faisant passer pour un préposé de sa banque dont le numéro s'est affiché utilise à sa demande le dispositif de sécurité personnalisé pour supprimer puis réinscrire des bénéficiaires de virement dans le but d'éviter justement des opérations de malveillance.

Quels sont les faits ?

Dans cette affaire, Monsieur J a 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 par un préposé de l'établissement lui demandant d'ajouter, grâce à ses données personnelles de sécurité, cinq personnes sur la liste des bénéficiaires des virements.

Or, Monsieur J, en l'absence de prise en charge du sinistre par la banque, a donc assigné la banque en remboursement de ces sommes.

Procédure pour laquelle la Cour d'appel de Versailles avait donné raison à Monsieur J et c'est dans ces circonstances que la banque avait formé un pourvoi.

La banque faisait grief à la cour d'appel d'avoir condamné l'établissement bancaire à payer à Monsieur J la somme de 54 500.00 € avec intérêts au taux légal ainsi que la somme de 1 500.00 € à titre de dommages et intérêts pour préjudice moral avec intérêts au taux légal.

Les pertes occasionnées par des opérations de paiement non autorisées.

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

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

La négligence grave du payeur.

Or, dans cette affaire, la cour d'appel avait relevé que, suivant ses opérations, 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 l'attaque informatique et qu'il fallait désormais les réenregistrer, 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 bénéficiaire, ce qu'il avait fait en saisissant son code confidentiel.

Pour autant, la banque reprochait à la cour d'appel d'avoir considéré qu'il ne s'agissait pas d'acte négligent que Monsieur J n'avait pas été gravement négligent en validant les opérations dont il n'était pas l'auteur alors qu'il aurait dû en vérifier toutes les données comme le rappelle au besoin l'article L133-19 du Code monétaire et financier rappelant que cet article précise :

> « *I. - 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 L133-17, les pertes liées à l'utilisation de cet instrument, dans la limite d'un plafond de 50 €.*
> *Toutefois, la responsabilité du payeur n'est pas engagée en cas :*
> - *d'opération de paiement non autorisée effectuée sans utilisation des données de sécurité personnalisées ;*
> - *de perte ou de vol d'un instrument de paiement ne pouvant être détecté par le payeur avant le paiement ;*
> - *de perte due à des actes ou à une carence d'un salarié, d'un agent ou d'une succursale d'un prestataire de services de paiement ou d'une entité vers laquelle ses activités ont été externalisées.*
>
> *II. - La responsabilité du payeur n'est pas engagée si l'opération de paiement non autorisée a été effectuée en détournant, à l'insu du payeur, l'instrument de paiement ou les données qui lui sont liées. Elle n'est pas engagée non plus en cas de contrefaçon de l'instrument de paiement si, au moment de l'opération de paiement non autorisée, le payeur était en possession de son instrument.*
> *III. - Sauf agissement frauduleux de sa part, le payeur ne supporte aucune conséquence financière si le prestataire de services de paiement ne fournit pas de moyens appropriés permettant l'information aux fins de blocage de l'instrument de paiement prévue à l'article L133-17.*
> *IV. - Le payeur supporte toutes les pertes occasionnées par des opérations de paiement non autorisées si 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 L133-16 et L133-17.*
> *V. - Sauf agissement frauduleux de sa part, le payeur ne supporte aucune conséquence financière si l'opération de paiement non autorisée a été effectuée sans que le prestataire de services de paiement du payeur n'exige une authentification forte du payeur prévue à l'article L133-44.*
> *VI. - Lorsque le bénéficiaire ou son prestataire de services de paiement n'accepte pas une authentification forte du payeur prévue à l'article L133-44, il rembourse le préjudice financier causé au prestataire de services de paiement du payeur* ».

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

La négligence grave du payeur et les opérations de paiements non autorisées.

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'indice permettant un utilisateur normalement attentif de douter de l'identité de son interlocuteur.

Pour autant, la cour d'appel a relevé que, suivant ses déclarations, Monsieur J avait été contacté par téléphone par l'issue d'une personne se présentant comme l'assistant de sa conseillère bancaire qui lui avait expliqué qu'il était nécessaire de supprimer des bénéficiaires de virement pour déjouer une attaque informatique et mobile, des messages l'invitant à valider des ajouts de bénéficiaire, ce que Monsieur J avait fait en saisissant son code confidentiel et qu'il lui avait été enfin expliqué qu'il n'aurait plus accès à son compte, qu'il allait recevoir par la poste un nouvel identifiant de compte et un nouveau mot de passe.

Un escroc se faisant passer pour le conseiller financier et détenteur d'informations confidentielles.

La cour d'appel avait effectivement retenu que Monsieur J n'avait pas été gravement négligent quant à l'identité de son interlocutrice qui prétendait être, non pas sa conseillère bancaire, mais l'assistance de celle-ci, l'objet de l'appel

qui tendait à réenregistrer des bénéficiaires de virement.

Opération qui pouvait pourtant se faire sans intervention d'une employée de la banque qui ne présentait au surplus aucune urgence dans la mesure où Monsieur J n'aurait plus accès à son compte en ligne pendant plusieurs jours et les explications qui lui avaient été fournis 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 soit adressés par voie postale, constituait, pour la banque, des indices permettant à un utilisateur normalement attentif de suspecter une fraude.

De telle sorte que, pour la banque, la cour d'appel n'avait pas tiré toutes les conséquences légales des dispositions de l'article L133-19 du Code monétaire et financier.

La banque finissant son raisonnement en considérant que, même de bonne foi, le payeur doit supporter toutes les pertes occasionnées par des opérations de paiement non autorisées si ces pertes résultent d'une négligence grave de sa part.

Le *spoofing* et l'usurpation d'identité.

Dès lors, pour la banque, l'utilisation d'un « *spoofing* » ou usurpation d'identité n'est pas une circonstance opérante, usurpation d'identité qui a mise Monsieur J en confiance et a diminué sa vigilance, ce qui n'était pas une circonstance suffisante pour excuser sa négligence qui était pourtant grave.

La Cour de cassation, fort heureusement, ne partage absolument pas son analyse.

La Haute juridiction vient consacrer dans un arrêt de principe qui, à mon sens, mérite une large diffusion dans lequel elle précise, qu'après avoir exactement énoncé qu'il incombait 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 apparaissant sur le téléphone portable de Monsieur J s'était affiché comme étant celui de Madame Y sa conseillère bancaire et retient qu'il croyait être en relation avec une salariée de la banque lors du réenregistrement et 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 assurait qu'il s'agissait d'une opération sécurisée.

Une mise en confiance du titulaire du compte bancaire.

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

La Cour de cassation considérant que, dès lors, la cour d'appel a pu en déduire que la négligence grave de Monsieur J n'était pas caractérisée et a donc très naturellement rejeté le pourvoi de l'établissement bancaire.

Une négligence grave non caractérisée.

Ainsi, cette jurisprudence est fort intéressante puisqu'elle vient finalement trancher une problématique relative à la définition même de la négligence grave au sens de l'article L133-19 du Code monétaire et financier qui amène finalement au titulaire du compte qui s'est finalement fait escroquer par un entretien téléphonique dans lequel il pensait échanger avec un responsable bancaire, ce qui l'avait d'ailleurs amené à baisser sa vigilance et se retrouver seul finalement à supporter les conséquences de cette escroquerie.

Or, la réalité est que si la baisse de vigilance est obtenue par ces tierces personnes c'est parce que justement celles-ci ont quand même entre les mains des informations à caractère confidentiel qu'elles ont sûrement obtenu sur le « *Darkweb* » à travers des informations qui, à un moment donné ou à un autre, échappés à l'établissement bancaire.

Des informations à caractère confidentiel échappant à la banque.

Dès lors, ce n'est qu'un juste retour des choses que de voir finalement la banque sanctionnée sur cette problématique de responsabilité bancaire car, s'il est vrai que le titulaire doit être prudent et attentif quant à la conservation et à la communication de ses informations confidentielles et de son dispositif de sécurité personnalisée, il n'en demeure pas moins que si Monsieur J a été « *endormi* » par un prétendu conseiller bancaire au téléphone, c'est bien évidemment sur la base d'informations confidentielles que ce dernier avait entre ses mains.

Ce qui laisse donc à penser que ses informations ont « *fuitées* » de l'établissement bancaire qui a donc quelque part, immanquablement, une part de responsabilité.

La sécurisation des données à caractère confidentiel par la banque.

Dès lors, cette jurisprudence est intéressante car effectivement tout démarre, à mon sens, sur une problématique de sécurisation des données bancaires par la banque elle-même qui voit ces informations fuitées pour être, par la suite, revendues sur le Darkweb, puis, exploitées par des personnes peu scrupuleuses qui vont se faire passer pour un banquier dans le cadre d'un entretien téléphonique visant justement à empêcher une escroquerie, baissant ainsi la vigilance du titulaire du compte bancaire qui, du coup, va réaliser des opérations qu'il n'aurait jamais réalisé en temps normal.

Un client avertissant toujours trop tard son établissement bancaire du *spoofing*.

Ce qui est d’autant plus intéressant c’est que, bien souvent, dans ce genre d’affaire très rapidement le titulaire du compte a tout de suite un doute et va immédiatement prévenir son établissement bancaire, parfois dans les minutes ou dans les dix minutes qui suivent, sans que pour autant la banque en tire toutes les conséquences car, le mal étant déjà fait, ces derniers ne cherchent pas ou n’ont pas les moyens de mettre fin à cette fuite financière et, par la suite, quand bien même le titulaire du compte s’est précipité auprès de l’établissement bancaire, quand bien même ce dernier les a immédiatement averti, dans la mesure où le mal est déjà fait, la banque se lave les mains de toute forme de responsabilité et vient finalement reprocher une négligence grave du titulaire pour s’exonérer de toute forme de responsabilité.

Fort heureusement, cette jurisprudence rappelle donc qu’aucune négligence grave au sens de l’article L133-19 du Code monétaire et financier ne peut être imputée au titulaire d’un compte qui est contacté téléphoniquement par une personne se faisant passer pour un préposé de sa banque dont le numéro s’est affiché utilise à sa demande le dispositif de sécurité personnalisé pour supprimer, puis, réinscrire les bénéficiaires de virement dans le but d’éviter des opérations malveillantes.

A bon entendeur….

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