Fraude bancaire : bataille légitime même pour les petits montants. Par Virginie Audinot, Avocat.

Parution : vendredi 28 février 2025

Adresse de l'article original :
https://www.village-justice.com/articles/fraude-bancaire-bataille-legitime-meme-pour-les-petits-montants,52504.html

Les décisions concernant les cas de fraude bancaire ne visent pas que des détournements de sommes importantes. Heureusement, les justiciables victimes de détournements moindres peuvent également obtenir gain de cause, de même qu'il leur faut en revanche compter d'avancer dans l'attente les frais de procédure y afférents.

La décision très récente du Tribunal judiciaire de Lille rendue à l'occasion d'une fraude bancaire (*fishing et spoofing*) sur un enjeu d'à peine plus de 2.000 euros est l'occasion de se pencher sur la question (TJ Lille, Chambre 10, 11 févr. 2025, n° 24/05705).

En l'espèce, la victime est titulaire d'un compte bancaire ouvert dans les livres de la banque CIC Nord Ouest.

Se prévalant d'opérations de paiement non autorisées du 3 mai 2023, la victime a déposé plainte auprès des services de police le 9 mai 2023 pour des faits d'escroquerie.

Par lettre du 10 mai 2023, elle a sollicité le remboursement des virements frauduleux, à savoir la somme totale de 2.125,97 euros.

Par lettre du 15 mai 2023, le CIC a accusé réception de sa réclamation, et, le 24 mai suivant, lui a répondu refuser le remboursement de la somme en question.

La victime a donc saisi le médiateur du CIC qui, par avis du 13 septembre 2023, a estimé que la responsabilité de la banque ne pouvait être engagée.

Compte tenu de la somme en jeu, inférieure à 5 000 euros, la victime a recouru à une procédure préalable de conciliation. Selon procès-verbal du 7 mai 2024, le conciliateur de justice a constaté l'échec de la tentative préalable de conciliation, le CIC ne s'étant pas présenté.

Il faut savoir que les banques sont particulièrement réticentes à rembourser les victimes de fraude bancaire tant qu'elles n'y sont pas enjointes par une décision de justice, et sont malheureusement bien souvent aux abonnés absents.

La victime n'a donc plus eu d'autre choix pour faire valoir ses droits que de saisir le tribunal judiciaire afin de voir condamner le CIC à lui payer la somme de 2.125,97 euros, assortie des intérêts au taux légal à compter de la requête, outre des frais de procédure et les dépens.

En l'espèce, la victime a expliqué avoir réalisé un paiement en ligne le 22 avril 2023 sur un site marchand coréen et payé des frais de douane le 2 mai 2023 pour recevoir son colis. Dès le lendemain, donc le 3 mai 2023, elle a reçu un appel d'un numéro d'urgence du CIC ([XXXXXXXX05]). L'interlocuteur s'est présenté être chargé de fraudes, collaborateur de la conseillère bancaire de la victime, et lui a indiqué que sa carte de paiement avait été piratée à l'occasion du paiement des frais de douane. Il s'agissait en réalité d'une personne usurpant cette qualité (méthode du « *spoofing* »).

Le fraudeur a invité la victime, via l'application bancaire, à valider le remboursement des trois paiements en ligne frauduleusement débités de son compte le 3 mai 2023, d'un montant de 750 euros, de 1.366,82 euros et de 9,15 euros. Après vérification du numéro de téléphone, et constatant qu'il s'agissait bien de celui de la banque, la victime s'est exécutée, pensant légitimement dialoguer avec sa banque.

Par la suite, elle a pris l'attache de son agence bancaire, qui l'a informée de la fraude dont elle venait en réalité d'avoir été victime.

La victime a contesté toute négligence grave, rappelant que le fraudeur avait usé d'une ligne téléphonique du CIC et qu'elle ne pouvait donc légitimement penser que la banque n'avait pas sécurisé le numéro de téléphone de sa plateforme. Elle a souligné en outre que le fraudeur avait également fait référence au nom de sa conseillère bancaire pour diminuer sa vigilance.

Enfin, elle a précisé que si le CIC l'a alertée le 12 juin 2023 sur l'existence de fraudes, la banque n'a en revanche changé son interface de paiement en ligne pour mettre en garde ses utilisateurs à chaque opération qu'à compter de février 2024.

La banque, de son côté, a soutenu, pour tenter de se défaire de son obligation de remboursement découlant des dispositions du Code monétaire et financier, que les opérations de paiement avaient été consenties au moyen d'un procédé d'authentification forte, à savoir la confirmation sur l'application bancaire de son téléphone portable des virements par saisie d'un code confidentiel, et que dès lors, face à une opération consentie, sa responsabilité ne peut pas être engagée et, *a fortiori*, qu'elle n'a pas à démontrer de négligence grave de l'utilisatrice pour s'en exonérer.

A titre subsidiaire, le CIC a ajouté que selon lui, la victime avait été doublement négligente en communiquant à l'escroc ses données personnelles par sms (*phishing*), à l'occasion du paiement des frais de douane, puis en validant les opérations sur son application bancaire (*spoofing*), pendant sa communication avec le fraudeur, et que celle-ci s'était exécutée alors que les notifications l'informaient clairement de l'exécution d'une opération de paiement. Enfin, le CIC a rappelé avoir mis en œuvre des moyens pour prévenir ces fraudes et diffuser des alertes à ses clients.

Le tribunal a tout d'abord rappelé les règles applicables en matière d'opération de paiement non autorisée.

Il résulte ainsi des articles L133-18 et L133-19 du Code monétaire et financier qu'en cas d'opération de paiement non autorisée, réalisée au moyen d'un instrument de paiement doté de données de sécurité personnalisées, et signalée par l'utilisateur dans les conditions prévues à l'article L133-24, le prestataire de services 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 L133-19.

L'article L133-19, II, du Code monétaire et financier précise que 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.

A l'inverse, le payeur supporte, en application de l'article L133-19, IV, du Code monétaire et financier, 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, qui l'oblige à prendre toute mesure raisonnable pour préserver la sécurité des données de sécurité personnalisées de son instrument de paiement, et L133-17, qui l'oblige à informer sans tarder le prestataire de service de paiement 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.

Dans son arrêt du 23 octobre 2024, la chambre commerciale de la Cour de cassation [1] a notamment jugé qu'aucune négligence grave ne pouvait être imputée au titulaire d'un compte qui, contacté téléphoniquement par une personne se faisant passer pour un préposé de sa banque dont le numéro s'affichait (*spoofing*), utilise à sa demande le dispositif de sécurité personnalisé pour supprimer puis réinscrire des bénéficiaires de virements dans le but d'éviter des opérations malveillantes.

Concernant les règles de preuve, la Cour de cassation juge, sur le fondement des articles L133-16, L133-17, L133-19, IV, et L133-23 du Code monétaire et financier, que s'il appartient à l'utilisateur de service 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 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**. Cette preuve ne peut se déduire du seul fait que l'instrument de paiement ou les données personnelles qui lui sont lies ont été effectivement utilisées [2].
Concernant l'authentification forte enfin, il ressort du Code monétaire et financier que, sous réserve de la fraude, 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. Ce dernier texte définit une authentification forte comme une authentification reposant sur l'utilisation de deux éléments ou plus appartenant aux catégories « *connaissance* », « *possession* » et « *inhérence* » et indépendants, en ce sens que la compromission de l'un ne remet pas en question la fiabilité des autres, conçue de manière à protéger la confidentialité des mesures d'authentification, et l'exige pour l'accès au compte de paiement en ligne, l'initiation d'une opération de paiement électronique et l'exécution d'une opération par le biais d'un moyen de communication à distance, susceptible de comporter un risque de fraude en matière de paiement ou de toute autre utilisation frauduleuse.

En l'espèce, trois opérations de paiement d'un montant de 750 euros, de 1.366,82 euros et de 9,15 euros, ont donc été débités du compte courant de la victime à son insu.

Le tribunal relève que si ces opérations ont été effectuées à l'issue d'un procédé d'authentification forte, elles n'ont pas, pour autant, été autorisées par le payeur, au sens des articles précités, tels qu'interprétés par la jurisprudence, lequel n'a pas consenti à leur montant, la victime ayant constamment agi pour obtenir un remboursement.

Les trois opérations de paiement constituant donc des opérations de paiement non autorisées, les juges ont décidé qu'il appartient à la banque de prouver la négligence grave de l'utilisateur des moyens de paiement.

Or, à cet égard, la victime justifiait, par capture d'écran de son téléphone portable, avoir été contacté par un numéro de téléphone correspondant à celui de la ligne d'urgence de la CIC pour faire opposition à sa carte bancaire.

La victime a expliqué aussi que le fraudeur avait fait usage d'une fausse qualité de conseiller bancaire du CIC ainsi que de l'identité de sa conseillère bancaire habituelle, pour l'amener à réaliser les opérations en ligne.

Concernant ensuite la confirmation de paiement réalisée par la victime sur son application en ligne, les juges ont souligné que même si le processus de confirmation mobile avait effectivement fait apparaître une demande de confirmation de paiement, et, en aucun cas, un remboursement ou une annulation de paiement, les manœuvres initiées par le fraudeur avaient en tout état de cause mis en confiance la victime et amoindri considérablement sa vigilance qui, face à la brièveté d'un appel téléphonique, dans un contexte d'anxiété générée par les allégations de piratage, ne disposait pas du temps nécessaire pour se renseigner et s'apercevoir des anomalies révélatrices de leur origine frauduleuse.

Aussi, dans ce contexte, les juges ont considéré, à juste titre, que la victime cliente bancaire du CIC n'avait pas commis de négligence grave et condamné la banque à rembourser à cette dernière la somme de 2.125,97 euros au titre des opérations de paiements non autorisées, assortie des intérêts au taux légal à compter de la requête, soit le 24 mai 2024, et aux dépens.

Virginie Audinot, Avocat Barreau de Paris Audinot & Associés www.fraude-bancaire.fr

[1] Cass. com., 23 octobre 2024, n° 23-16.627.

[2] Com. 18 janvier 2017, n°15-18.102.