BACAGe
ISSN : 3036-7824
Éditeur : UGA Éditions

06 | 2026

Droit au remboursement de l'utilisateur de services de paiement victime de *spoofing*

Stéphane Zinty

https://publications-prairial.fr/bacage/index.php?id=1485

DOI : 10.35562/bacage.1485

Référence électronique
Stéphane Zinty, « Droit au remboursement de l'utilisateur de services de paiement victime de *spoofing* », *BACAGe* [En ligne], 06 | 2026, mis en ligne le 15 juin 2026, consulté le 15 juin 2026. URL : https://publications-prairial.fr/bacage/index.php?id=1485

Droits d'auteur
CC BY-SA 4.0

Prairial
Pôle éditorial
Lyon Saint-Étienne

Droit au remboursement de l'utilisateur de services de paiement victime de *spoofing*

Stéphane Zinty

DOI : 10.35562/bacage.1485

Droits d'auteur
CC BY-SA 4.0

DÉCISION DE JUSTICE

CA Grenoble, ch. civile – N° 24/01962 – 25 novembre 2025

PLAN

TEXTE

1. Contexte

1 La fraude au faux conseiller bancaire ou *spoofing* est un phénomène en pleine expansion. Elle s'inscrit dans le cadre d'une mutation des fraudes bancaires vers des techniques de manipulation psychologique consistant à usurper l'identité d'un conseiller bancaire pour amener la victime à valider des opérations. Cette évolution des pratiques frauduleuses fait elle-même écho au renforcement des règles de protection du consentement de l'utilisateur de services de paiement à travers la généralisation de l'authentification forte. Des montants significatifs sont aujourd'hui concernés avec une multiplication des litiges entre les banques et leurs clients au sujet du remboursement. Un contentieux important s'est ainsi fait jour ayant amené la chambre commerciale de la Cour de cassation, dans un arrêt fondamental du 23 octobre 2024[1], à affirmer que la victime de

spoofing ne s'est pas systématiquement rendue coupable d'une négligence grave en validant les opérations frauduleuses et doit alors être remboursée. Pour autant, les litiges se multiplient devant les juges du fond, lesquels ont l'occasion d'appliquer, voire de préciser la solution posée par la Haute Cour. L'arrêt rendu par la cour d'appel de Grenoble le 25 novembre 2025 s'inscrit pleinement au sein du contentieux émergent de la fraude au faux conseiller bancaire.

2. Solution

2 Une cliente de la banque ING a été contactée à deux reprises, les 17 et 20 mars 2022, par une personne se présentant comme un conseiller de sa banque. Le numéro affiché sur son téléphone correspondait au véritable numéro de la banque ING, grâce à une technique permettant d'usurper l'identité téléphonique d'un tiers. L'interlocuteur annonça de façon pressante à la cliente l'existence de tentatives de fraude sur son compte, tout en la rassurant et en lui indiquant prendre avec elle les mesures de sécurité nécessaires pour empêcher cette fraude en cours. Deux virements furent ainsi immédiatement exécutés, pour un montant total de 10 000 euros (8 500 euros puis 1 500 euros) vers un compte appartenant à un tiers. La cliente indiqua alors qu'elle n'était pas à l'origine de ces virements et le signala formellement le 7 avril 2022 à sa banque ING au moyen de son application bancaire avant de déposer une plainte pour vol et usurpation d'identité. Elle réclama ensuite le remboursement de la somme de 10 000 euros auprès de sa banque laquelle refusa au motif d'une négligence grave.

3 Par acte de commissaire de justice en date du 12 décembre 2022, la cliente assigna alors sa banque devant le tribunal judiciaire de Grenoble. Par jugement en date du 6 mai 2024, ce dernier la débouta de sa demande de condamnation de la société ING Bank France au paiement de la somme de 10 000 euros, de sa demande de dommages et intérêts pour manquement à l'obligation de vigilance, ainsi que de sa demande de dommages et intérêts au titre de la responsabilité extra contractuelle. Le jugement la condamna également à payer à la société ING Bank la somme de 2 500 euros au titre de l'article 700 du Code de procédure civile. Appel fut en conséquence interjeté le 24 mai 2024 devant la cour d'appel de Grenoble.

4 La banque soutint pour sa part en appel que sa cliente avait validé l'ajout du bénéficiaire ainsi que les deux virements concernés à la suite de la réception par SMS des codes d'accès renforcés (authentification forte), si bien que les opérations avaient été authentifiées, dûment enregistrées et qu'elles n'avaient pas été affectées d'une déficience technique. Par ailleurs, la banque lui reprocha une négligence en n'ayant pas pris toutes les mesures nécessaires afin de préserver la confidentialité de ses données de sécurité personnalisées, alors que les SMS reçus indiquaient en capital la mention « attention, ne transmettez à personne ce code ». Enfin, la banque estima que l'action en responsabilité initiée par sa cliente pour défaut de vigilance ne saurait prospérer dans la mesure où seul le régime de responsabilité prévu par la Code monétaire et financier est applicable en matière de paiement à l'exclusion du droit commun.

5 Dans un arrêt en date du 25 novembre 2025, la cour d'appel de Grenoble considère que la banque, sur la base des logs informatiques produits, rapporte la preuve que les opérations litigieuses ont été authentifiées, dûment enregistrées et qu'elles n'ont pas été affectées d'une déficience technique ou autre, si bien qu'elles ont volontairement été exécutées par sa cliente. Toutefois, le numéro d'appel apparaissant sur le téléphone portable de celle-ci lors des opérations frauduleuses était celui de la banque « de sorte que l'utilisation de ce mode opératoire du spoofing [...] a mis Mme [J] en confiance s'agissant d'un appel émanant prétendument de sa banque, l'alertant sur un possible piratage de ses comptes et la rassurant quant aux mesures prises pour éviter que cette tentative n'aboutisse ». Il s'ensuit que la négligence grave de Mme [J] n'est pas caractérisée sur le fondement des articles L. 133-19 IV et L. 133-23 al. 2^{e} du Code monétaire et financier « de sorte qu'elle est bien fondée à réclamer paiement à la société ING Bank de la somme de 10 000 euros correspondant au montant total frauduleusement prélevé sur son compte bancaire » selon l'article L. 133-18 du même Code.

3. Appréciation

6 La décision de la cour d'appel de Grenoble intervient dans un contexte où malgré la solution posée par la Cour de cassation le 23 octobre 2024 le contentieux demeure encore instable et se concentre sur la qualification de l'opération (autorisée ou non) et le comportement du client (négligence grave ou non). En la matière, il s'avère que les juges grenoblois ont strictement appliqué et même précisé la position de la Haute Cour.

7 En effet, si le principe du droit au remboursement en cas de paiement non-consenti, posé par l'article L. 133-18 du Code monétaire et financier, est exclu en cas de fraude ou de négligence grave du client [2], les contours de la notion de négligence grave interrogent en présence d'une fraude au faux conseiller bancaire. Alors que l'on sait que l'utilisation des données personnelles du client ne prouve pas la négligence grave [3], dans quelle mesure peut-on dire du client ayant lui-même validé les opérations frauduleuses qu'il n'a pas été négligent ? À l'instar de la Cour de cassation ayant affirmé que la vigilance du client est nécessairement affaiblie dans les conditions caractéristiques du *spoofing* par rapport à une situation d'hameçonnage [4], la cour d'appel de Grenoble relève que « l'utilisation du mode opératoire du *spoofing* permettant aux fraudeurs d'afficher un numéro de téléphone qui n'est pas le leur mais le vrai numéro de la banque, a mis Mme [J] en confiance […], l'alertant sur un possible piratage de ses comptes et la rassurant quant aux mesures prises pour éviter que cette tentative n'aboutisse ». Dès lors, sauf circonstances particulières, la fraude au faux conseiller s'accompagne nécessairement d'un contexte spécifique altérant la vigilance du client et excluant en principe sa négligence grave.

8 Les juges grenoblois apportent une précision supplémentaire à cette solution à propos de son articulation avec le processus d'authentification forte requis par l'article L. 133-4 du Code monétaire et financier, issu de l'ordonnance n° 2017-1252 du 9 août 2017 portant transposition de la directive 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015. La preuve par la banque de l'authentification, de la comptabilisation et de l'absence de déficience technique des opérations litigieuses [5] en particulier par un procédé

d'authentification forte, bien qu'elle soit devenue un préalable nécessaire à la caractérisation de la négligence grave [6], ne suffit pas à démontrer cette dernière lorsque le contexte révèle une manœuvre de fraude sophistiquée reposant sur l'ingénierie sociale et l'usurpation de numéros bancaires. Sévère pour les banques, la solution a vocation à protéger les utilisateurs des services de paiement afin de maintenir un niveau de confiance suffisant dans l'actuel système de paiement [7]. Un rééquilibrage a été toutefois été opéré par la Cour de cassation, laquelle, reprenant la jurisprudence de la Cour de justice de l'Union européenne [8], a pu affirmer que dès lors que la responsabilité d'un prestataire de services de paiement est recherchée en raison d'une opération de paiement non autorisée ou mal exécutée, seul est applicable le régime de responsabilité défini aux articles L. 133-18 à L.133-24 du Code monétaire et financier, à l'exclusion de tout régime alternatif de responsabilité résultant du droit national [9]. Cette solution n'est nullement contredite en l'espèce par la cour d'appel de Grenoble qui rend sa décision au visa des règles spécifiques du droit des opérations de paiement issues du Code monétaire et financier et non celles issues du droit commun.

9 Enfin, il convient de ne pas oublier que la réponse jurisprudentielle au *spoofing*, au sein de laquelle s'inscrit l'arrêt d'appel commenté, s'accompagne plus largement d'une reconfiguration du droit des opérations de paiement afin de répondre plus efficacement à ce phénomène. En effet, la loi Naegelen n° 2020-901 du 24 juillet 2020 impose aux opérateurs téléphoniques un contrôle renforcé de l'origine des appels, en rendant obligatoire l'authentification des numéros appelants lors des communications sortantes qui passent par un réseau IP et utilisant le protocole SIP [10]. Par ailleurs, en application du règlement UE 2024/886 du 13 mars 2024, les prestataires de services de paiement, depuis le 9 octobre 2025 pour ceux situés dans un État membre dont la monnaie est l'euro [11], ont l'obligation de vérifier en matière de virement la concordance entre le nom du destinataire et celui du titulaire de l'IBAN bénéficiaire afin d'attirer l'attention du client sur un risque de fraude [12]. De même, la loi n° 2025-1058 du 6 novembre 2025 a renforcé l'arsenal anti-fraude, notamment au moyen d'un nouvel article L. 521-6-1 du Code monétaire et financier instaurant un fichier national des comptes signalés pour risque de fraude, géré par la

Banque de France, qui recense certains comptes de paiement ou de dépôt estimés susceptibles d'être frauduleux. Cette loi organise aussi un meilleur partage d'informations entre acteurs habilités. Le *spoofing*, vecteur majeur de la fraude au virement, est donc incontestablement un phénomène pris très au sérieux par les autorités.

NOTES

1 Cass. com., 23 octobre 2024, nº 23-16267. Dans le même sens, Cass. com., 12 juin 2025, nº 24-13777.

2 CMF, art. L. 133-23 al. 2e.

3 CMF, art. L. 133-23 al. 2e. Cass. com., 18 janvier 2017, nº 15-18102 ; Cass. com., 28 mars 2018, nº 16-20018.

4 Cass. com., 23 octobre 2024, nº 23-16267, préc. : « Le mode opératoire par l'utilisation du *spoofing* a mis M. [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 de davantage de temps pour s'apercevoir d'éventuelles anomalies révélatrices de son origine frauduleuse. »

5 CMF, art. L. 133-23, al. 1er.

6 Cass. com., 12 novembre 2020, nº 19-12112 ; Cass. com., 20 novembre 2024, nº 23-15099 ; Cass. com., 30 avril 2025, nº 24-10149.

7 Voir N. Kilgus, « L'évolution des procédures de contestations des paiements », *RDBF* 2018, nº 2, dossier 11.

8 CJUE, 16 mars 2023, aff. C-351/21.

9 Cass. com, 27 mars 2024, nº 22-21200.

10 CPCE (Code des postes et des communications électroniques), art. L. 44 IV.

11 PE et cons. UE, règl. nº 2012/260, 14 mars 2012, art. 5 quater, § 9.

12 J. Lasserre Capdeville, « Droit des opérations de paiement : présentation du règlement européen nº 2024/886 du 13 mars 2024 intéressant les virement instantanés », *GPL*, 28 mai 2024, nº GPL463t1, spéc. nº 23 et suiv.

RÉSUMÉ

Français
Ne commet pas une négligence grave la cliente d'une banque validant, en application d'un procédé d'authentification forte, des virements frauduleux dans les circonstances caractéristiques d'une fraude au faux conseiller bancaire.

INDEX

Mots-clés
banque, paiement, authentification forte, fraude, faux conseiller bancaire, négligence grave, remboursement

Rubriques
Droit des affaires

AUTEUR

Stéphane Zinty
Maître de conférences, Univ. Grenoble Alpes, CRJ, 38000 Grenoble, France
stephane.zinty[at]univ-grenoble-alpes.fr
IDREF : https://www.idref.fr/184687071
ISNI : http://www.isni.org/0000000448711389