



Victimes de phishing : quels recours judiciaires?

Conseils pratiques publié le **18/12/2024**, vu **96 fois**, Auteur : [JURISOFIA - Contentieux - Responsabilité, Bancaire, Travail, Immo.](#)

Les victimes d'escroqueries ou phishing peuvent engager des actions judiciaires contre les banques pour obtenir réparation, en prouvant l'absence de négligence grave ou en invoquant leur obligation de sécurité renforcée.

Si la médiation échoue ou si la banque refuse de rembourser, le consommateur peut engager une action judiciaire.

Une attention particulière doit être apportée au délai de prescription pour agir en justice: les délais peuvent être longs devant le médiateur (plus ou moins volontairement) et le délai de prescription, non suspendu dans ce cas, peut arriver à terme entre temps.

1. Saisine d'une juridiction

Saisine du **Tribunal judiciaire ou de proximité** : Selon le montant du préjudice.

Action collective : En cas de fraude massive affectant plusieurs clients d'une même banque, une action de groupe peut être envisagée (article L. 623-1 du Code de la consommation).

Attention à la notion de **faute ou négligence grave du consommateur** qui permet d'éviter d'aboutir à la responsabilité de la banque.

La notion de négligence grave est centrale dans les litiges liés aux opérations bancaires frauduleuses, notamment dans les cas de phishing ou d'escroqueries.

Elle est interprétée par la jurisprudence et la doctrine comme un comportement de l'utilisateur de services bancaires manifestant un manque évident de prudence, dépassant la simple imprudence ou inadvertance. Comment cette notion est abordée :

1.1. Définition doctrinale de la négligence grave

- Un comportement objectivement déraisonnable au regard des standards attendus d'un utilisateur de services bancaires.
- Une violation des règles élémentaires de prudence, comme la communication volontaire de données confidentielles ou la réponse à des courriels suspects.

Pour autant, elle n'exige pas une intention frauduleuse ou complice de la part de l'utilisateur, mais seulement un manquement manifeste à ses obligations de vigilance.

Avis de la doctrine sur l'équilibre des responsabilités

Certaines analyses doctrinales soulignent que la notion de négligence grave est parfois **utilisée pour transférer la charge du risque au consommateur**, ce qui peut aller à l'encontre des principes de protection de la clientèle fixés par le Code monétaire et financier et la directive PSD2.

1.2. Interprétation jurisprudentielle

- **Décisions favorables aux banques**
 - o Cass. civ. 1ère, 8 mars 2012, n° 10-23.321 : La Cour de cassation a estimé que le client qui communique volontairement ses codes confidentiels en réponse à un message frauduleux commet une négligence grave justifiant le refus de remboursement par la banque.
 - o CA Paris, 13 septembre 2018, n° 17/13835 : L'absence de vérification d'un courriel suspect avant de répondre a été considérée comme une négligence grave de la part du consommateur.
- **Décisions favorables aux consommateurs** (*postérieures donc évolution ? Vers une faveur pour les consommateurs ?*)
 - o Cass. civ. 1ère, 25 mars 2021, n° 19-12.681 : La négligence grave ne peut être invoquée par la banque si celle-ci n'a pas mis en œuvre des systèmes de sécurité adéquats, tels que l'authentification renforcée.
 - o CJUE, arrêt du 25 janvier 2023 (C-287/22) : La Cour de justice de l'Union européenne a rappelé que la négligence grave ne peut être retenue lorsque le consommateur a été manipulé dans un contexte rendant son erreur compréhensible.

Critères déterminants en jurisprudence

- **Comportement de l'utilisateur** : Communication de données sensibles ou manque de vigilance

Exemples récents :

Plusieurs décisions récentes de jurisprudence illustrent la tendance des tribunaux à condamner les banques à rembourser leurs clients victimes de phishing ou de spoofing, même lorsque ces dernières invoquent une « négligence grave » de la part des clients.

- Cour de cassation, 23 octobre 2024 (n°23-16.267): Dans une affaire impliquant la BNP Paribas, un client victime d'une fraude dépassant 50 000 euros a obtenu gain de cause après un pourvoi de la banque. La **Cour a retenu que la banque devait prouver concrètement la négligence grave du client**, notamment dans des cas où le spoofing (c'est-à-dire d'usurpation d'identité) réduit la vigilance de la victime. Ce jugement impose une responsabilité accrue aux banques dans la protection contre les fraudes sophistiquées?[1]
- Cour d'appel de Versailles, 2023 : Un arrêt de la Cour d'appel a confirmé le remboursement d'un client piégé par une opération frauduleuse validée via une application sécurisée. La décision souligne que la manipulation psychologique par le spoofing peut annuler l'argument de négligence grave avancé par la banque. Ici aussi, la banque a été reconnue responsable pour ne pas avoir sécurisé suffisamment ses systèmes?
- CJUE, arrêt du 25 janvier 2023 (C-287/22) : La Cour de justice de l'Union européenne a rappelé **l'obligation de remboursement des opérations non autorisées, même si le consommateur a été imprudent, à moins que la négligence grave soit prouvée.**

Ces jugements montrent une interprétation stricte par les tribunaux des obligations de sécurité incombant aux banques, notamment en matière de fraude liée aux nouvelles technologies. Les clients sont invités à signaler rapidement toute opération suspecte et à demander conseil pour faire valoir leurs droits.

2. Assistance des associations de consommateurs

Des organismes comme UFC-Que Choisir ou 60 Millions de Consommateurs peuvent accompagner les victimes dans leurs démarches, y compris dans la constitution d'un dossier de plainte contre la banque.

Pour défendre efficacement vos droits et explorer les recours adaptés face à des litiges bancaires, notre cabinet vous accompagne à chaque étape, en mettant à votre service son expertise et une stratégie personnalisée.

[1] <https://www.village-justice.com/articles/arnaque-par-spoofing-cour-cassation-condamne-banque-rembourser-client,51237.html>