

Les arnaques en ligne et les obligations des établissements bancaires : un enjeu crucial pour la protection des consommateurs. Par Dorian-Jacob Le Bay, Juriste.

Parution : mardi 31 décembre 2024

Adresse de l'article original :

<https://www.village-justice.com/articles/arnaque-ligne-banques-queelles-sont-les-obligations-des-etablissements-bancaires,51816.html>

Reproduction interdite sans autorisation de l'auteur.

Les arnaques en ligne, telles que le *phishing* ou le *smishing*, exploitent la vulnérabilité des consommateurs pour accéder à leurs données bancaires. Face à cette recrudescence de fraudes, les établissements bancaires ont des obligations légales de prévention, d'information et de sécurisation des transactions.

Avec la numérisation croissante des services financiers, les arnaques en ligne connaissent une recrudescence, exploitant la vulnérabilité des consommateurs et les failles potentielles des systèmes bancaires. Parmi les stratagèmes les plus fréquents figurent le *phishing*, le *vishing*, le *smishing* ou encore le *spoofing* qui visent à extorquer les coordonnées bancaires des victimes par des moyens frauduleux. Ce contexte soulève deux questions majeures : quelles sont les obligations des établissements bancaires en matière de prévention des fraudes et quelles sont leurs responsabilités en cas d'opérations frauduleuses ?

I. Les obligations préventives des établissements bancaires.

A. La mise en place de systèmes de sécurité adaptés.

Les établissements bancaires sont tenus par une obligation de moyen renforcée en matière de sécurité, en vertu de la Directive (UE) 2015/2366 sur les services de paiement (« DSP2 »). [1] Cette directive impose notamment l'authentification forte (à deux facteurs) pour les transactions en ligne (article 97 de la DSP2), une mesure essentielle pour limiter les risques de fraude.

L'article 22 du règlement d'exécution (UE) 2018/389 [2] précise les exigences techniques applicables à l'authentification forte des clients, notamment l'utilisation de dispositifs générant des codes uniques et des systèmes de surveillance des transactions suspectes.

Par ailleurs, l'article L561-10 du Code monétaire et financier [3] impose aux banques de mettre en place des dispositifs internes pour prévenir les risques de fraude et de blanchiment, incluant des outils de détection automatique des anomalies.

En doctrine, plusieurs auteurs insistent sur le rôle de la technologie dans la prévention des fraudes bancaires. Ainsi, en 2021, Y. Serra [4] insistait déjà sur la nécessité des banques d'investir dans des solutions d'intelligence artificielle capables d'analyser en temps réel les comportements anormaux.

B. Analyse de l'article L561-10 du Code monétaire et financier.

L'article L561-10 du Code monétaire et financier constitue une pierre angulaire dans l'édifice juridique de la lutte contre la fraude, le blanchiment de capitaux et le financement du terrorisme. Ce texte impose aux établissements financiers une responsabilité de premier plan : celle d'élaborer et de maintenir des dispositifs internes rigoureux, conçus pour préserver l'intégrité du système financier. Cette exigence, qui s'inscrit dans une dynamique européenne et internationale, transcende la simple application législative pour embrasser une vision globale de sécurité et de transparence.

Sous l'impulsion de cet article, les établissements financiers sont tenus de développer des mécanismes sophistiqués et adaptés à la complexité croissante des menaces financières.

Parmi ces dispositifs, plusieurs se distinguent par leur importance stratégique :

Les systèmes de surveillance automatisée des transactions : ces derniers reposent sur des technologies avancées, notamment l'intelligence artificielle et les algorithmes prédictifs, qui permettent de détecter en temps réel des opérations suspectes. Leur finalité est de signaler des anomalies, telles que des virements incompatibles avec le profil du client ou des transactions répétées dans des juridictions à risque.

Les procédures de vigilance à l'égard des clients (KYC) : la vigilance renforcée est au cœur des obligations imposées par le législateur. Elle implique l'identification rigoureuse des clients et de leurs bénéficiaires effectifs, ainsi qu'une attention particulière aux personnes politiquement exposées (PEP). Ce dispositif repose sur l'idée selon laquelle la transparence dans les relations contractuelles est la première ligne de défense contre les dérives financières.

La déclaration de soupçon à Tracfin : les établissements sont investis d'un devoir d'alerte. En vertu de l'article L561-15 du CMF [5] toute transaction suspectée d'être liée à des activités illicites doit être déclarée à Tracfin. Ce mécanisme, conçu pour briser l'opacité des circuits financiers, témoigne de la nécessaire collaboration entre les entités privées et les autorités publiques.

Les contrôles internes renforcés : l'arrêté du 6 janvier 2021 [6] détaille les modalités d'audit interne et de formation continue des personnels bancaires, plaçant les organes de direction au centre des responsabilités. Ce cadre ambitieux vise à institutionnaliser une culture de la conformité au sein des établissements financiers.

Ces systèmes reposent sur des technologies avancées, notamment l'intelligence artificielle et les algorithmes prédictifs, qui permettent de détecter en temps réel des opérations suspectes. Leur finalité est de signaler des anomalies, telles que des virements incompatibles avec le profil du client ou des transactions répétées dans des juridictions à risque. Ces outils, véritable vigie numérique, s'inscrivent dans une logique préventive et proactive.

C. L'information et l'éducation des clients.

Les banques ont également une obligation d'information prévue par l'article L312-1-1 du Code monétaire et financier [7] Cette obligation implique de fournir aux clients des informations claires et compréhensibles sur les risques liés à l'utilisation des services de paiement, ainsi que sur les mesures de sécurité à adopter.

Des campagnes de sensibilisation (via courriels, SMS, ou plateformes bancaires en ligne) alertant sur les dernières tendances en matière de fraude complètent cette mission. La jurisprudence souligne que la carence de la banque dans cette mission peut être constitutive d'une faute engageant sa responsabilité contractuelle [8].

Sur ce point, R. Perrot [9] évoque une évolution vers une obligation proactive, qui va au-delà de la simple transmission d'informations pour inclure des conseils personnalisés selon le profil de risque du client. Cela signifie que le devoir d'information s'élargit pour inclure une véritable dimension de conseil, tenant compte des caractéristiques individuelles du client et de sa situation particulière (et non uniquement d'une information pouvant être jugée trop généraliste).

II. Les responsabilités des banques en cas de fraude.

Le législateur n'a laissé aucune ambiguïté quant aux sanctions encourues en cas de manquement aux obligations prévues par l'article L561-10 du Code monétaire et financier. Ces mesures, qui mêlent sanction administrative, responsabilité civile et impact réputationnel, illustrent la gravité des enjeux :

Les sanctions administratives : l'Autorité de contrôle prudentiel et de résolution (ACPR) dispose d'un large pouvoir répressif. Elle peut infliger des amendes de plusieurs millions d'euros, limiter les activités des établissements défaillants, voire en suspendre l'agrément.

La responsabilité civile : les banques peuvent être tenues responsables des préjudices subis par leurs clients ou des tiers en raison d'un manquement à leurs obligations de vigilance. Cette responsabilité, qui repose sur le principe de la faute, engage directement l'image et la pérennité des institutions financières concernées.

L'impact réputationnel : au-delà des sanctions formelles, la défaillance en matière de lutte contre le blanchiment ou la fraude peut porter un coup sévère à la réputation de l'établissement. Dans un secteur où la confiance est primordiale, une telle atteinte peut s'avérer dévastatrice.

A. La prise en charge des opérations frauduleuses.

Le droit positif prévoit des garanties solides pour les victimes de fraudes bancaires. En vertu de l'article L133-18 du Code monétaire et financier [10], les banques doivent procéder au remboursement immédiat des opérations non autorisées, sauf preuve d'une **négligence grave** imputable au client ou si ce dernier a participé à la fraude.

L'article 11 de la DSP2 confirme cette disposition, en précisant que les prestataires de services de paiement doivent rétablir sans tarder la situation financière du client concerné. Cependant, cette obligation est subordonnée à la diligence du client dans la notification de la fraude (généralement dans un délai de 13 mois, article L133-24 du CMF [11]).

Si la faute du client est avérée, une franchise limitée à 50 euros peut être appliquée conformément à l'article L133-19 du CMF [12] À l'inverse, l'absence de vigilance suffisante de la banque engage sa responsabilité pleine et entière.

En cas de désaccord, le client peut saisir le médiateur bancaire après avoir épuisé les voies internes de résolution (réclamation adressée au conseiller bancaire, et en cas de réponse insatisfaisante, au service client de la banque). Ce recours, accessible et normé, vise à garantir une solution équitable et rapide aux différends.

Si la solution proposée par le médiateur ne vous satisfait pas, vous avez la possibilité de porter l'affaire devant la justice. Le recours au médiateur suspend le délai de deux ans prévu pour saisir la justice. Ce délai recommence à courir dès que le médiateur communique sa proposition de solution.

La juridiction compétente varie en fonction du montant en litige :

Pour un litige de 10.000 euros ou moins, il s'agit du tribunal de proximité ou du tribunal judiciaire.

Pour un litige excédant 10.000 euros, seul le tribunal judiciaire est compétent (avec représentation par avocat obligatoire).

B. La charge de la preuve.

Selon l'article L133-23 du Code monétaire et financier [13] il appartient à la banque de démontrer que l'opération contestée a été valablement authentifiée, enregistrée et correctement exécutée. La jurisprudence renforce cette position en rappelant que les preuves apportées par la banque doivent être indiscutables [14].

En cas d'échec à apporter une preuve satisfaisante, l'établissement bancaire est tenu de rembourser les sommes frauduleusement prélevées, ainsi que les frais associés [15].

C. La notion de négligence grave.

Le concept de négligence grave demeure une zone grise du droit bancaire. La jurisprudence a considéré que la divulgation involontaire de ses données bancaires par la victime, lorsqu'elle a été trompée par un stratagème sophistiqué, ne constitue pas systématiquement une négligence grave [16] En principe, cette appréciation doit être

faite *in concreto*, aux circonstances de l'espèce. [17] Pour autant, d'autres arrêts se réfèrent à un « *utilisateur normalement attentif* » [18].

Pour autant, les tribunaux ont tendance à interpréter de manière stricte la notion de négligence grave afin de ne pas pénaliser davantage les victimes déjà lésées [19].

III. La jurisprudence : l'arrêt du 23 octobre 2024 comme repère.

La jurisprudence récente éclaire les contours des obligations pesant sur les établissements financiers. L'arrêt n° 23-16.267 de la Cour de cassation, rendu le 23 octobre 2024 [20] apporte une clarification essentielle sur la notion de négligence grave dans un contexte de fraude.

Dans cette affaire, un client avait été victime d'une fraude par *spoofing*, une technique d'usurpation d'identité particulièrement sophistiquée. Ayant cru légitimement communiquer avec sa banque, il avait autorisé plusieurs virements frauduleux. Saisie du litige, la Cour a estimé que la preuve de la négligence grave incombe au prestataire de services de paiement, et non au client. En l'espèce, l'affichage du numéro usurpé avait renforcé la crédibilité de l'interlocuteur frauduleux, exonérant ainsi le client de toute responsabilité.

Cet arrêt souligne l'impérieuse nécessité pour les banques de renforcer leurs mécanismes de détection et de prévention. Il illustre également la montée en puissance des attentes du juge à l'égard des établissements financiers face à des menaces toujours plus complexes.

Conclusion.

Les arnaques en ligne représentent un véritable défi pour les consommateurs et les établissements bancaires. Si les obligations préventives imposées par la DSP2 et le Code monétaire et financier ont permis de renforcer les dispositifs de sécurité, elles doivent être accompagnées d'un effort constant de sensibilisation des clients.

Par ailleurs, la jurisprudence récente, notamment l'arrêt du 23 octobre 2024, révèle les implications pratiques de ces dispositifs et rappelle aux établissements bancaires leur responsabilité accrue face à des fraudes toujours plus sophistiquées, sous réserve des exceptions prévues par la loi. Dès lors, il apparaît impératif d'investir dans des systèmes de prévention robustes, tout en informant davantage les consommateurs à la prudence nécessaire dans leurs interactions avec les services financiers.

À l'heure où la confiance est le socle de toute relation bancaire, la mise en œuvre rigoureuse des mesures prévues par l'article L561-10 du Code monétaire et financier constitue bien plus qu'une obligation légale : elle est le garant de la pérennité des institutions financières elles-mêmes et demeure la clé pour répondre aux défis croissants en matière de lutte contre la criminalité financière.

En bref.

Les arnaques en ligne (*phishing*, *smishing*, *spoofing*, etc.) sont de plus en plus fréquentes et visent à voler les données bancaires des consommateurs. Face à ces fraudes, les banques ont des obligations légales pour sécuriser les transactions, informer leurs clients et détecter les anomalies.

Les obligations des banques.

Sécurisation des paiements : les banques doivent utiliser des systèmes de protection avancés, comme l'authentification à deux facteurs, pour limiter les fraudes.

Détection des fraudes : elles doivent surveiller les opérations suspectes grâce à des outils comme l'intelligence artificielle.

Information des clients : les banques ont l'obligation de sensibiliser leurs clients aux risques d'arnaques et de leur fournir des conseils pratiques.

En cas de fraude, quels sont vos droits ?

Remboursement des sommes volées : si vous signalez rapidement une fraude (dans un délai de 13 mois), votre banque doit vous rembourser, sauf si elle prouve une négligence grave de votre part.

Recours en cas de désaccord :

Réclamation interne : contactez votre conseiller ou le service client de votre banque.

Médiateur bancaire : si la réponse ne vous satisfait pas, vous pouvez saisir le médiateur de votre banque gratuitement.

Justice : s'il y a lieu, portez l'affaire devant le tribunal compétent.

Dorian-Jacob Le Bay Juriste - Legal Designer Doctorant en droit bancaire et financier Droit des affaires : droit de la distribution bancaire, droit des assurances, droit du numérique et droit des entreprises en difficulté [->dorian-jacob.lebay@objectifprojet.fr]

[1] Directive (UE) 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur.

[2] Règlement délégué (UE) 2018/389 de la Commission du 27 novembre 2017 complétant la directive (UE) 2015/2366 du Parlement européen et du Conseil par des normes techniques de réglementation relatives à l'authentification forte du client et à des normes ouvertes communes et sécurisées de communication.

[3] Article L561-10 du Code monétaire et financier.

- [4] Y. Serra. (2021). La sécurité des paiements électroniques : enjeux et perspectives, Revue Banque.
- [5] Article L561-15 du Code monétaire et financier.
- [6] Arrêté du 6 janvier 2021 relatif au dispositif et au contrôle interne en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme et de gel des avoirs et d'interdiction de mise à disposition ou d'utilisation des fonds ou ressources économiques.
- [7] Article L312-1-1 du Code monétaire et financier.
- [8] Cass. com., 5 avril 2023, n° 21-22.300.
- [9] Revue trimestrielle de droit commercial.
- [10] Article L133-18 du Code monétaire et financier.
- [11] Article L133-24 du Code monétaire et financier.
- [12] Article L133-19 du Code monétaire et financier.
- [13] Article L133-23 du Code monétaire et financier.
- [14] CA Amiens, 1re ch. civ., 7 avril 2017, n° 15/02794.
- [15] CA Douai, 8e ch., 1re sect., 3 nov. 2016, n° 16/00233.
- [16] CA Douai, 8e ch., 1re sect., 3 nov. 2016, n° 16/00233.
- [17] Cass. com., 25 oct. 2017, n° 16-11.644.
- [18] Cass. com., 28 mars 2018, n° 16-20.018.
- [19] CA Douai, 3e ch., 5 janvier 2023, n° 21/04625.
- [20] Cass. com., 23 oct. 2024, n° 23-16.267.
-