

Fraude bancaire : la protection des consommateurs renforcée par la jurisprudence

Au sein de notre société numérisée, les techniques toujours plus perfectionnées de fraude bancaire constituent un fléau croissant qui génère des pertes considérables. Ces évolutions nécessitent une adaptation continue de la protection des utilisateurs.



Par M^{me} Valérie Godé, avocat au Barreau de Grenoble et médiateur inscrit auprès de la cour d'appel de Grenoble.

Les banques se retrouvent en effet au cœur d'une importante difficulté entre la protection des fonds qui leur sont confiés, celle du consommateur, et leur obligation de vigilance. La jurisprudence récente tend à renforcer les obligations pesant sur les établissements bancaires. Cette évolution s'inscrit dans un mouvement plus large de protection accrue des consommateurs de services financiers dans un contexte de fraudes de plus en plus élaborées.

L'accroissement des obligations et de la responsabilité des établissements bancaires

Le dispositif législatif ne cesse d'être contraint d'évoluer afin de faire face à la progression des techniques de fraude, et la jurisprudence témoigne d'un renforcement progressif des obligations pesant sur les professionnels du secteur bancaire. Le législateur français et européen quant à lui est contraint d'adapter les textes au fur et à mesure, pour répondre rapidement aux nouvelles techniques frauduleuses.

La loi du 6 novembre 2025 renforce les dispositifs de lutte contre la fraude au paiement Sepa et contre la fraude au chèque. Elle prévoit la création d'un mécanisme de partage d'informations entre les prestataires de services de paiement sous la forme d'un fichier national des comptes signalés pour risque de fraude (FNC-RF). Ce mécanisme est de nature à renforcer la lutte contre la fraude au virement et la fraude au prélèvement, qui représentent un préjudice de 334 millions d'euros en 2023.

Il ressort des articles 133-15 et L 133-38 du Code monétaire et financier une répartition des responsabilités entre les établissements bancaires et les utilisateurs de services de paiement. La directive européenne DSP2, transposée en droit français en 2018, a considérablement renforcé les obligations de sécurité imposées aux banques et a instauré l'authentification forte pour les opérations électroniques. Dans

un arrêt du 30 août 2023 (Com. 30 août 2023, n° 22-11707), la Cour de cassation a posé le principe que, 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 n'exige une authentification forte prévue par l'article L. 133-4 du Code monétaire et financier.

La responsabilité des établissements bancaires constitue un principe composant le droit bancaire français. Ce n'est pas un mécanisme fondé sur la faute, mais il vise à engager la responsabilité de l'établissement bancaire indépendamment de toute négligence prouvée. Cette protection confirmée par la Cour de cassation par un arrêt du 25 octobre 2017 (Cass.com. 25 octobre 2017, n° 16-10.170), vise à garantir une indemnisation des victimes et à inciter les banques, et néobanques en ligne, à renforcer leurs systèmes de sécurité. Ce pourvoi posait la question du caractère autorisé d'une opération de paiement initiée par le payeur donnant un ordre de paiement par l'intermédiaire du bénéficiaire à qui il avait transmis par téléphone le numéro de sa carte bancaire et le cryptogramme y étant associé, ainsi que l'obligation pour l'établissement de crédit d'exiger dans cette hypothèse l'authentification forte.

L'arrêt du 28 mars 2018 (Cass. com., n° 16-20.018) constitue une référence en la matière, ayant précisé que l'obligation de sécurité de la banque ne saurait être limitée par une clause contractuelle exonératoire de responsabilité. Cette décision s'inscrit dans une tendance jurisprudentielle favorable aux consommateurs victimes de fraudes.

En tout état de cause, « la négligence grave », limite à la protection du consommateur

La protection du consommateur connaît des limites prévues par l'article L 133-15 du Code de la consom-

Lorsque la fraude repose sur un mécanisme de tromperie élaboré, impliquant une usurpation d'identité, connaissance d'informations internes et absence de signes manifestes de danger, la responsabilité du client ne peut être retenue.

mation, lorsque le client a fait preuve de « négligence grave » ou « a agi frauduleusement ». La Cour de cassation, dans son arrêt du 12 novembre 2020 (Cass. 12 novembre 2020, n° 19-12.112), a refusé de qualifier de négligence grave la situation de fraude dans laquelle un client a été victime de techniques de phishing particulièrement sophistiquées. Longtemps, les banques ont tenté de donner une définition très large de la notion de « négligence grave ». Or, la jurisprudence évolue et tend aujourd'hui à limiter l'utilisation de « la négligence grave » aux cas où le client a fait preuve d'une négligence manifeste, volontairement, et sans intervention frauduleuse.

En résumé, la protection du consommateur est consacrée par le Code monétaire et financier, car :

- La responsabilité des banques est présumée en cas d'opération non autorisée par le client,
- Le client bénéficie d'un régime de preuve favorable,
- La charge de la négligence grave du client visée par l'article L 133-15 du Code monétaire et financier incombe à l'établissement financier.

Phishing, spoofing et utilisation de faux conseillers bancaires

La protection des utilisateurs des services de paiement concernant des situations de fraude spécifiques, comme le phishing (ou hameçonnage via SMS ou mail frauduleux), le spoofing (usurpation d'identité via adresse mail, IP, numéro de téléphone) et l'utilisation de faux conseillers bancaires, est accrue. Allant plus loin, par un arrêt récent du 12 juin 2025, la Cour de cassation (Cass Com. 12 juin 2025 n° 24-13.777) confirme une position protectrice à l'égard des utilisateurs de services de paiement victimes de fraudes sophistiquées. Selon cet arrêt, la négligence grave demeure une notion d'interprétation stricte, et il incombe au prestataire de services de paiement d'en rapporter la preuve.

Lorsque la fraude repose sur un mécanisme de tromperie élaboré, impliquant une usurpation d'identité, connaissance d'informations internes et absence de signes manifestes de danger, la responsabilité du client ne peut être retenue.

La Cour de justice européenne a même établi que les clauses contractuelles faisant peser sur le consommateur la charge de prouver l'absence de négligence sont abusives. La Cour de cassation est allée jusqu'à retenir la responsabilité d'un établissement bancaire dont le dispositif d'authentification présentait des failles exploitées par les fraudeurs. Par un arrêt récent du 20 novembre 2024, la Cour de cassation a rendu un arrêt clé en matière de responsabilité des utilisateurs d'instruments de paiement et des obligations des banques en cas d'opérations de paiement non autorisées (Cass Com. 20 nov. 2024 n° 23-15.099) : cette jurisprudence impose des contrôles rigoureux aux banques avant d'imputer les pertes à leurs clients. Ainsi, le consommateur se trouve protégé par la jurisprudence, dans un contexte de développement des néobanques et de multiplication des techniques de fraudes bancaires toujours plus sophistiquées (phishing, spoofing).

En ce qui concerne la jurisprudence relative aux faux investissements, la responsabilité des établissements bancaires peut être engagée sur la base d'un manquement à leur obligation de vigilance. Par exemple, si les virements sont anormalement élevés, répétitifs ou incohérents par rapport à l'historique du compte, repose ici sur la banque l'obligation d'avertir le client. Les juges prennent en considération la crédibilité de scénario frauduleux, par exemple lorsque l'escroc utilise le téléphone de la banque ou connaît des informations personnelles du client. La jurisprudence considère que le fait d'avoir été dupé n'est pas suffisant pour justifier un refus de remboursement de la part de l'établissement bancaire.

Ces arrêts récents montrent que les banques devront renouveler d'efforts pour établir la traçabilité des opérations et prévenir les litiges en renforçant leurs dispositifs de sécurité afin de garantir la sécurité des fonds confiés à elles en confiance par le consommateur. Subsiste cependant un flou jurisprudentiel, concernant certaines formes de fraudes particulièrement sophistiquées, comme les faux investissements ou le phishing. ●