Financité

FÉDÉRATION WALLONIE-BRUXELLES

ARNAQUES BANCAIRES DE BIEN LENTES AVANCÉES POUR LES VICTIMES

PLUSIEURS AVANCÉES LÉGALES SONT À L'ÉTUDE

ANNE FILY - SEPTEMBRE 2026

Résumé

Cette analyse montre que les victimes belges de phishing bancaire supportent l'essentiel des pertes financières (92%), les banques invoquant systématiquement le « consentement » technique de la victime pour refuser tout remboursement. Une jurisprudence récente commence toutefois à inverser cette logique en exigeant que les banques remboursent avant d'enquêter, tendance que confirment plusieurs propositions législatives belges et le futur règlement européen sur les services de paiement (RSP), qui redéfinit l'opération « autorisée » autour du consentement réel de la personne et responsabilise davantage les banques.

Introduction

La numérisation des opérations de paiement a ouvert la porte à de nouvelles formes de criminalité de masse. Près de la moitié de la population de notre pays a été confrontée au phishing (hameçonnage) et 6,8 % ont été directement victimes[1]. Une récente étude menée dans quinze pays européens montre que les Belges figurent parmi les plus touché·e·s et les plus susceptibles d'être arnaqué·e·s plusieurs fois[2].

Cela ne semble pas prêt de s'arrêter si l'on en croit le dernier message d'alerte de Safewonweb (juillet 2026)[3] : le phishing par téléphone (appelé vishing[4]), associé ou non à un mail, voire à une visite à domicile, est en augmentation.

Il semble néanmoins que les chiffres rendus publics sont bien en deçà de la réalité : le nombre de victimes de pratiques de phishing qui rapportent les faits auprès des services de police ne dépasserait pas les 21 %[5], les personnes concernées ressentent souvent de la honte et ne font pas état de ce qu'il leur est arrivé[6].

Alors que les montants détournés par ce biais sont très élevés (quelque 49 millions d'euros en 2024)[7], les coûts du phishing sont pour l'essentiel supportés par les victimes (92 % du préjudice subi), et pas par les banques[8]. La numérisation des opérations de paiement s'est traduite par un important transfert de responsabilité en matière de sécurité sur les épaules des consommateur rice s, ce qui n'était pas le cas quand les opérations de paiement étaient effectuées en agence.

1 Traitement actuel des plaintes des victimes

1.1 La victime a-t-elle autorisé l'opération de paiement contestée ?

La victime ne serait-elle pas responsable de ce qui lui arrive dans la plupart des cas ? C'est en tout cas l'interprétation que font les banques de la législation actuellement en vigueur.

[1] Moniteur de sécurité 2024, Police fédérale, 2024 https://www.police.be/statistiques/sites/statspol/files/statistics_files_upload/VMS%20Archive/11_VMS%202024/VMS_2024_fr/01_F%C3%A9d%C3%A9ral/02_Tendances/Analyse_Moniteur_de_s%C3%A9curit%C3%A9_2024.pdf (page 36)

[2] L'Echo, *Escroqueries: les Belges figurent parmi les Européens qui perdent le plus d'argent*, 09/06/2026, https://www.lecho.be/monargent/banque-et-assurances/escroqueries-les-belges-figurent-parmi-les-europeens-qui-perdent-le-plus-d-argent/10674509.html

[3] Safewonweb, *Tendances du Phishing en 2026 : repère les dernières arnaques*, 26/07/2026, https://safeonweb.be/fr/actualite/tendances-du-phishing-en-2026-repere-les-dernieres-arnaques

[4] Voir description en annexe

[5] Voir note 1

[6] Moran Garcia S., *Les Belges victimes de fraude en ligne ont honte: «Le silence rend les autres plus vulnérables»*, 08/04/2026, https://www.levif.be/economie/mon-argent/les-belges-victimes-de-fraude-en-ligne-ont-honte-le-silence-rend-les-autres-plus-vulnerables/

[7] Febelfin, Chiffres 2024: *Si ça ressemble à du phishing, c'est probablement du phishing !,* 04/08/2025, https://febelfin.be/fr/themes/fraude-et-securite/chiffres-et-tendances/chiffres-2024-si-ca-ressemble-a-du-phishing-c-est-probablement-du-phishing

[8] Fily A., Kubicki M., Arnaques bancaires : qui est responsable ? Financité, 09/2025, https://www.financite.be/sites/default/files/references/images/Arnaques%20bancaires-AFMK-septembre2025.pdf

Mais que dit la loi ? Selon l'art. VII.32 du Code de droit économique[9]:

« *§ 1er. Une opération de paiement est réputée autorisée si le payeur a donné son consentement à l'exécution de l'ordre de paiement. (…)*
§ 2. Le consentement à l'exécution d'une opération de paiement ou d'une série d'opérations de paiement est donné sous la forme convenue entre le payeur et le prestataire de services de paiement et conformément à la procédure convenue. (…) En l'absence de consentement, l'opération de paiement est réputée non autorisée.
(…)
§ 4. La procédure de consentement fait l'objet d'un accord entre le payeur et le ou les prestataires de services de paiement concernés. »

Les banques estiment que la notion de consentement est une question purement technique : si la personne qui conteste le virement a respecté la procédure de validation des paiements prévue par sa banque, c'est la preuve qu'elle a donné son consentement au paiement. Dans la plupart des cas, les victimes ont effectivement communiqué leurs identifiants personnalisés aux escrocs ou effectué eux-mêmes les virements frauduleux en les validant par exemple via l'application Itsme. Sur la base de cette interprétation extrêmement stricte de la législation, l'opération est considérée comme autorisée. Pour les banques, aucun remboursement n'est donc possible. Peu importent les circonstances, et notamment le fait que l'escroc se soit fait passer pour un employé de la banque et ait eu recours à toutes les formes de manipulation psychologique pour extorquer de l'argent à sa victime.

Pour Ombudsfin, le médiateur des services financiers[10], il y a lieu de faire la différence entre les opérations librement et consciemment acceptées par la victime et celles qui ne le sont pas, les premières étant considérées comme autorisées, les secondes ne l'étant pas et doivent faire l'objet d'un remboursement.

Il n'y a pas d'opération autorisée lorsque la victime transmet par téléphone, sur instruction du fraudeur, le code généré à l'aide de sa carte bancaire, de son code PIN ou de son digipass. La victime n'est pas nécessairement informée que ce code permet de confirmer une opération de paiement et elle ne connaît généralement pas le montant ni le bénéficiaire de l'opération. De la même manière, si la victime saisit ce code sur un site web frauduleux ou sur un appareil contrôlé par l'escroc, l'objectif de l'action est caché par l'escroc.

De la même manière, dans le cas d'une prise de contrôle par l'escroc d'un appareil via un logiciel comme Anydesk ou Teamviewer ou via une application frauduleuse, la victime ne voit généralement pas ce que le fraudeur fait réellement sur son appareil. Elle ne voit souvent qu'un écran noir, un message d'erreur ou un message similaire. En outre, le digipass de la victime n'affiche pas toujours des informations détaillées sur le montant et le bénéficiaire (cela dépend du type de digipass). Dans ces circonstances, Ombudsfin estime qu'il s'agit d'opérations de paiement non autorisées et que la victime doit être remboursée.

En revanche, lorsqu'un·e escroc demande par téléphone à la victime d'effectuer elle-même un virement vers un compte prétendument sécurisé et que la victime encode et confirme elle-même le virement dans son environnement bancaire en ligne, il s'agit d'une opération de paiement autorisée. Pour Ombudsfin, bien que la victime soit trompée, elle connaît le montant et le numéro de compte du bénéficiaire et les saisit elle-même dans son environnement bancaire en ligne. Dans ces circonstances,

[9] Transposition en droit belge en 2018 de la Directive européenne sur les services de paiement n° 2015/2366 (PDS2)

[10] La contestation d'opérations à la suite d'un vishing constitue depuis plusieurs années le thème le plus important traité par Ombudsfin, le service de médiation en matière financière. Voir rapports annuels : https://www.ombudsfin.be/fr/publications/rapports-annuels

le consentement de la victime à l'exécution du virement est donc établi. Il n'y a donc pas lieu à remboursement.

Pour certains juristes, comme Laurent Frankignoul,[11] la position défendue par les banques revient à considérer que les opérations qui ont fait l'objet d'une procédure « d'authentification forte », comme lorsque l'on valide l'opération avec l'application Istme ou un digipass, sont nécessairement réputées autorisées. La thèse des banques reviendrait finalement à imposer à la victime d'apporter la preuve qu'elle n'a pas donné son consentement. Or le Code de droit économique prévoit que lorsqu'un e client e conteste avoir autorisé une opération, c'est à la banque qu'il revient de prouver que cette personne a donné son accord à l'opération de paiement et que, pour ce faire, « *l'utilisation d'un instrument de paiement, telle qu'enregistrée par le prestataire de services de paiement (…) ne suffit pas nécessairement en tant que telle à prouver que l'opération de paiement a été autorisée par le payeur (…)* » (art. VII. 42 CDE).

1.2 La victime a-t-elle fait preuve d'une négligence grave ?

Même dans les situations où il est admis que la victime n'a pas autorisé l'opération de paiement, cela ne veut pas dire pour autant qu'elle a automatiquement droit à un remboursement. Il faut aussi vérifier si elle était en capacité de détecter la fraude à l'avance et, dans l'affirmative, si elle n'a commis une négligence grave.

L'article VII.44, §1, alinéa 2, 1° du Code de droit économique prévoit que la victime ne supporte aucune perte si la perte, le vol ou l'utilisation abusive de son instrument de paiement n'ont pas pu être constatés par la victime avant que l'opération n'ait été effectuée.

Pour Ombudsfin, la communication de codes par téléphone (y compris les codes de réponse générés par digipass), l'utilisation d'Itsme ou d'une application bancaire sur instruction téléphonique pour « annuler » des opérations (alors que les messages visibles dans itsme et l'application bancaire sont clairs) et le fait d'autoriser un tiers à prendre le contrôle de l'environnement bancaire en ligne sur l'appareil de la victime via des applications logicielles telles qu'Anydesk ou Teamviewer sont des actes qui vont tellement à l'encontre de l'obligation pour le payeur de garantir la sécurité de ses instruments de paiement et de leurs données de sécurité personnelles, prévue à l'article VII.38§2 du CDE, qu'ils peuvent être constitutifs de négligence grave. Dans ce cas, la banque n'est pas tenue d'intervenir pour compenser le préjudice financier subi par la victime.

Ombudsfin précise toutefois que cette constatation générale ne l'empêche pas d'examiner les circonstances concrètes et factuelles de la fraude dans chaque dossier individuel soumis à son examen et de parvenir, le cas échéant, à une autre conclusion. Ombudsfin déclare vérifier aussi si la banque a agi avec suffisamment de diligence en matière de détection de la fraude et de récupération des fonds. Malheureusement, les banques ont rarement tenu compte de ces éléments pour intervenir même partiellement dans le remboursement de la victime.

Le 29 juin 2026, la Cour de cassation a cassé un jugement qui refusait d'indemniser un client de KBC au motif d'une négligence grave. Le principe de négligence grave n'est pas défini clairement dans la législation, il doit être déterminé par le juge au cas par cas, en tenant compte des éléments propres à chaque situation. La Cour de cassation a apporté un peu de clarté en définissant la notion de négligence grave comme suit : « *il y a négligence grave lorsque le payer adopte un comportement, ou s'abstient d'adopter un comportement, qu'un payeur raisonnable, normalement prudent et diligent, n'aurait pas*

[11] Frankignoul L. avocat spécialiste en droit bancaire, La notion d'opération de paiement « non autorisée », 08/10/2025, https://laurentfrankignoul.be/2025/10/08/la-notion-doperation-de-paiement-non-autorisee/

adopté ou n'aurait jamais omis d'adopter. »[12] Selon les commentateurs de cet arrêt[13], les termes utilisés par la Cour de cassation invitent à une lecture restrictive : il faut établir qu'un payeur raisonnable, normalement prudent et diligent, n'aurait jamais agi de la même manière. Il reste à voir comment les tribunaux appliqueront cette définition aux faits qui leur seront soumis.

1.3 La victime a-t-elle droit à un remboursement immédiat ?

Le Code de droit économique prévoit qu'en cas de paiement non autorisé, les banques doivent rembourser les victimes au plus tard le lendemain. Dans la pratique, les banques estiment qu'elles doivent d'abord faire une enquête, laquelle aboutit le plus souvent à considérer que la victime a autorisé l'opération et donc à refuser tout remboursement. La banque Belfius, détenue à 100% par l'Etat belge, a même osé inscrire dans ses conditions générales qu'elle ne remboursait les victimes qu'après une enquête sur une possible fraude ou négligence grave de la part du payeur. Sous pression, la banque a fini par modifier ses conditions générales.

Certaines victimes, qui ont parfois perdu toutes leurs économies, hésitent alors à entamer des actions en justice qui impliquent d'engager des frais supplémentaires alors qu'elles estiment que leurs chances de gagner sont faibles. Selon une avocate en droit bancaire, les banques comptent sur le fait que les victimes ne vont pas aller plus loin[14]. Un professeur en droit bancaire rappelle que c'est à la banque qu'il revient de prouver que la victime a donné son accord à l'opération de paiement et que, pour ce faire, « l'utilisation d'un instrument de paiement, telle qu'enregistrée par le prestataire de services de paiement (…) ne suffit pas nécessairement en tant que telle à prouver que l'opération de paiement a été autorisée par le payeur (…) » (art. VII. 42 CDE). Selon ce juriste, la thèse soutenue par le secteur bancaire entraîne ainsi rien de moins qu'un renversement de la charge de la preuve instituée par le Code de droit économique.

Le 2 juin dernier, le juge des référés d'Anvers a condamné une banque à rembourser immédiatement près de 50 000 euros à un couple victime de phishing. Le juge a en effet estimé que déterminer si une transaction a été autorisée ou non ne peut se faire en un jour. En attendant que cette enquête soit menée, la banque doit donc, à titre provisoire, rembourser le client[15]. Ce juge s'est basé sur un arrêt de la Cour de justice européenne (CJCE) établissant que les banques doivent toujours indemniser les victimes de phishing. Ce n'est qu'ensuite, si la banque estime que le client a commis une négligence grave, qu'elle peut engager une procédure pour récupérer l'argent[16]. Pour les juristes qui ont commenté ces décisions, les rôles sont désormais inversés : la banque doit d'abord payer et ensuite

[12] Cour de Cassation, Hof van Cassatie van België, https://hofvancassatie.be/pdf/arresten-arrets/C.25.0390.N.pdf

[13] Wery E., *Fraude: la Cour de cassation définit la « négligence grave » du payeur*, 29/07/2026, https://blog.oeccbb.be/fr/article/fraude-la-cour-de-cassation-definit-la-negligence-grave-du-payeur/32004

[14] Warland M., *Les banques sont obligées d'indemniser leurs clients victimes de phishing" : une décision juridique met le secteur bancaire sous pression*, RTBF, 04/06/2026, https://www.rtbf.be/article/phishing-les-banques-pourraient-passer-a-la-caisse-11734360?fbclid=IwY2xjawThWJBwZG9mAWV4dG4DYWVtAjEwAHNydGMGYXBwX2lkEDIyMjAzOTE3ODgyMDA4OTIAAR5D5BAxk0PJ8V-WAO82BuD7_emqxhCGoXROhKHlIBgb26RMf5sa9rU858UMNg_aem_vOYg6fOYBGe-n339eFY1Ig

[15] *Un précédent « révolutionnaire » : les banques doivent toujours indemniser les victimes de phishing, selon un juge*, Le Soir, 03/06/2026, https://www.lesoir.be/750575/article/2026-06-03/un-precedent-revolutionnaire-les-banques-doivent-toujours-indemniser-les / https://www.nieuwsblad.be/binnenland/banken-moeten-slachtoffers-van-phishing-meteen-terugbetalen-maar-belfius-zegt-zwart-op-wit-dat-zij-dat-niet-doen/156359932.html

[16] Cour de justice, 11 juillet 2024, C-409/22, Eurobank Bulgaria, ECLI:EU:C:2024:600, §§ 60-61

saisir elle-même les tribunaux pour contester cette indemnisation.

Une affaire pendante devant la CJCE pourrait définitivement clarifier cette question. L'avocat général, dont l'avis est généralement suivi par la Cour, a précisé dans ses conclusions[17] que même si la banque soupçonne une négligence grave, la banque doit d'abord rembourser et contester ensuite : « *Ce remboursement n'est donc pas définitif, mais il doit intervenir et, dans un second temps, si la banque établit que le client a manqué, délibérément ou par négligence grave, à l'une des obligations liées notamment aux données de sécurité personnalisées, elle peut lui demander de supporter les pertes correspondantes. Si le client refuse de rembourser le montant de l'opération non autorisée, il appartient à la banque d'engager une action en justice contre lui pour obtenir le paiement*. » Selon l'avocat général, une telle approche est justifiée par « *le libellé de la réglementation européenne en la matière, par le contexte dans lequel s'inscrivent les dispositions pertinentes identifiées par la juridiction nationale, et par la nécessité d'assurer un niveau élevé de protection des consommateurs utilisant des services de paiement, lequel constitue l'un des objectifs poursuivis par cette réglementation* ».

2 Travaux législatifs en cours

Le sort que les banques réservent aux victimes de phishing qui n'ont, en toute connaissance de cause, jamais consenti à se délester de leurs économies auprès d'escrocs, suscite une forte indignation et un grand mécontentement au sein de la société.

Même si la jurisprudence récente laisse un peu plus d'espoir aux victimes, il est évident que la législation actuelle qui découle de la transposition de la directive européenne sur les services de paiements de 2015 (PSD2) n'est pas du tout adaptée aux formes sophistiquées des escroqueries récentes. Or cette législation avait pourtant pour objectif de mieux protéger les consommateur·ice·s face aux risques de sécurité accrus liés aux paiements électroniques. C'est ce texte qui a par exemple introduit le principe de l'authentification forte qui s'applique lorsque l'on consulte son compte en ligne ou lorsque l'on initie un paiement électronique en ligne. A ce texte, malheureusement devenu obsolète, est venu s'ajouter le peu de considération des banques pour les victimes. Des modifications législatives sont donc envisagées pour y remédier tant au niveau national qu'européen.

2.1 Propositions d'amendements du Code de droit économique

Deux propositions de loi[18] sont actuellement sur la table de la Chambre des représentants, l'une déposée en 2024 par Anders et l'autre en 2026 par Vooruit.

Les deux textes proposent de préciser ce qu'est une opération de paiement autorisée en ajoutant les termes « lui-même » à l'Art. VII.32.1 § 1er du Code de droit économique : « *Une opération de paiement est réputée autorisée si le payeur a lui-même donné son consentement à l'exécution de l'ordre de paiement.* ». Selon les rédacteurs de ces deux textes, une opération de paiement sera en revanche réputée autorisée si la fraude consiste à convaincre par la ruse la victime de donner elle-même l'ordre de paiement. Cette précision correspond à la distinction admise par Ombudsfin et certains tribunaux,

[17] *Conclusion de l'avocat général,* M. Athanasios Rantos, Affaire C-70/25, 05/03/2026, https://www.droit-technologie.org/wp-content/uploads/2026/03/conclusions-avocat-general-1.pdf

[18] Proposition de loi modifiant plusieurs articles du Livre VII du Code de droit économique en vue de mieux protéger le payeur contre certaines formes de fraude déposée par V. Van Quickenborne (Anders) le 27/11/2024, https://www.lachambre.be/FLWB/PDF/56/0542/56K0542001.pdf
Proposition de loi modifiant le Code de droit économique en ce qui concerne la protection du payeur en cas d'opérations de paiement non autorisées résultant du phishing déposée par J. Soete (Vooruit) le 02/06/2026, https://www.lachambre.be/FLWB/PDF/56/1592/56K1592001.pdf

même si, juridiquement parlant, elle n'apporte rien de plus.

Le texte de Vooruit traite aussi de la question du délai de remboursement de la victime et propose de compléter l'Art. VII.43.§ 1er par les alinéas suivants :

« Une présomption de négligence grave de la part du payeur ne constitue pas un motif permettant de refuser ou de suspendre le remboursement immédiat par le prestataire de services de paiement.

"Si le prestataire de services de paiement refuse ou suspend le remboursement immédiat – qu'il qualifie l'opération d'autorisée ou de non autorisée – il en informe l'utilisateur de services de paiement au plus tard le dixième jour ouvrable suivant la réception de la notification visée à l'article VII.41, sans frais et sur papier ou sur un autre support durable.

Les informations à fournir à l'utilisateur de services de paiement dans cette notification comportent au moins les éléments suivants concernant :

1° les motifs spécifiques et la justification de la décision de refus ou de suspension, en précisant dans des termes aisément compréhensibles et sous une forme claire et intelligible si le refus ou la suspension est fondé sur le caractère autorisé ou non autorisé, ou sur une fraude de la part du payeur ;

2° les pièces justificatives techniques relatives à l'authentification et à l'enregistrement de l'opération contestée ;

3° une justification démontrant comment le prestataire de services de paiement s'est acquitté de son devoir général de diligence et comment son système de détection des fraudes a fonctionné par rapport à cette opération ;

4° la responsabilité du payeur conformément à l'article VII.44, y compris des informations sur le montant concerné ;

5° les voies de réclamation et de règlements extrajudiciaires des litiges ouvertes à l'utilisateur de services de paiement, conformément au livre XVI, y compris l'adresse physique de l'instance où l'utilisateur de services de paiement peut adresser ses réclamations, parmi lesquelles l'organisme compétent visé à l'article VII.216 et les coordonnées de la Direction générale Inspection économique auprès du SPF Économie." »

Cette proposition prend en compte la jurisprudence récente qui impose de rembourser la victime immédiatement quelles que soient les circonstances de la fraude : on rembourse d'abord, on enquête ensuite. La seule dérogation à cette obligation de remboursement concerne les cas de soupçon de fraude de la part de la victime (situation plutôt rare). La banque aurait alors l'obligation d'en informer le SPF Economie par écrit.

Si la banque décide malgré tout de suspendre le remboursement ou de ne pas rembourser parce qu'elle considère que la victime a fait preuve de négligence grave, elle doit dans les dix jours communiquer à cette dernière les éléments de preuve qui fondent sa décision et les voies de recours qui lui sont ouvertes. Par ailleurs, la banque qui tarderait à effectuer le remboursement se verrait infliger des intérêts de retard.

Les amendements proposés par Vooruit sont assez proches des dispositions du futur règlement européen sur les services de paiement en ce qui concerne les justificatifs du refus, les informations à fournir à la victime et les délais pour le faire.

Si le Code de droit économique devait être amendé, ce qui à ce jour n'a encore rien de certain, il en résultera une amélioration du sort d'une partie des victimes, amélioration qui reste toutefois cantonnée à ce que permet la transposition de la PSD2. Pour un changement plus radical, c'est au niveau européen qu'il faut agir.

2.2 Proposition de règlement européen sur les services de paiement

En 2023, la Commission européenne a proposé un « paquet législatif » relatif aux services de paiement comprenant :

- une directive[19] qui traite en gros des questions d'agrément, de supervision et du cadre institutionnel applicable aux établissements de paiement ;
- un règlement sur la sécurité des paiements (RSP)[20] avec pour objectif d'harmoniser directement (c'est-à-dire sans passer par la phase de transposition au niveau national) les règles de conduite, de transparence, d'authentification, de droits des utilisateurs, de mesures antifraude et de responsabilité.

La proposition initiale de la Commission européenne a été largement amendée tant par le Parlement européen que par le Conseil sur la question de la protection des victimes de fraude comme le montre le texte de compromis négocié entre le Conseil et le Parlement européen[21].

Le RSP reconnaît explicitement que les fraudes par ingénierie sociale brouillent la distinction entre transactions autorisées et non autorisées, puisque les fraudeurs peuvent prendre le contrôle de l'ensemble du processus de consentement et d'authentification forte[22]. Le RSP considère que la protection ne peut plus se limiter aux seules transactions non autorisées.

Une opération autorisée sera dans l'avenir définie autour du consentement du payeur : « *Une transaction de paiement ne sera pas considérée comme autorisée lorsque la transaction a été initiée ou modifiée par un tiers agissant sans le consentement de l'utilisateur du service de paiement, y compris en utilisant les identifiants de sécurité personnalisés de l'utilisateur du service de paiement obtenus frauduleusement* ». Le texte précise qu'une opération techniquement authentifiée y compris par le biais d'une authentification forte, enregistrée avec précision, saisie dans les comptes et non affectée par une panne technique ou une autre défaillance du service fourni, ne suffit pas à prouver que le consentement du payeur était juridiquement valable. Les circonstances dans lesquelles le payeur a donné son consentement doivent être prises en compte notamment en cas de manipulation par un escroc.

La victime qui a été manipulée par un tiers se faisant passer pour sa banque doit informer sa banque et porté plainte auprès des autorités nationales compétentes (police). La banque doit alors le rembourser intégralement et sans délai.

La banque peut toutefois mener une enquête avant de rembourser s'il soupçonne de la part de la victime, sur la base de motifs objectivement justifiés, une fraude (rare), un manquement intentionnel ou une négligence grave dans la protection de ses instruments de paiement ou ses données de sécurité. Dans ce cas, la banque ne peut pas simplement refuser le remboursement sans justification. La banque doit inviter la victime à fournir à l'appui de sa réclamation toute information ou preuve pertinente

[19] Proposition de directive du Parlement européen et du Conseil concernant les services de paiement et les services de monnaie électronique dans le marché intérieur, modifiant la directive 98/26/CE et abrogeant les directives (UE) 2015/2366 et 2009/110/CE, https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:52023PC0366

[20] Proposition de Règlement du Parlement européen et du Conseil concernant les services de paiement dans le marché intérieur et modifiant le règlement (UE) nº 1093/2010, https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:52023PC0367

[21] https://law-tracker.europa.eu/procedure/2023_210?lang=fr
Parlement européen : https://www.europarl.europa.eu/news/fr/press-room/20251121IPR31540/accord-sur-les-services-de-paiement-plus-de-protection-contre-la-fraude

[22] Authentification forte : authentification qui repose sur l'utilisation de deux éléments ou plus appartenant aux catégories « connaissance » (quelque chose que seul l'utilisateur connaît), « possession » (quelque chose que seul l'utilisateur possède) et « inhérence» (quelque chose que l'utilisateur est)

concernant les circonstances concrètes de l'opération contestée : complexité de la fraude, moyens utilisés, profil de la victime, avertissements émis par la banque, mesures de prévention mises en place et vulnérabilité potentielle de la victime. Cette approche protège la victime sans pour autant la dégager de toute responsabilité individuelle. Le RSP reconnait ainsi que les fraudes actuelles n'affectent pas seulement les personnes imprudentes, mais aussi les personnes âgées, les jeunes, les personnes moins à l'aise avec le numérique, tout comme des client e s averties confronté e s à de nouvelles pratiques frauduleuses extrêmement sophistiquées.

Lorsque la banque mène une enquête, elle doit, dans un délai de quinze jours ouvrables après avoir été saisie d'une réclamation, soit rembourser la victime, soit lui indiquer les motifs et éléments justifiant le refus de remboursement et indiquer les organismes ou voies de recours qu'elle peut saisir si elle conteste ce refus. Lorsque la banque refuse un remboursement après avoir conclu à l'issue de son enquête à une fraude de la part de la victime présumée, elle doit aussi en communiquer les motifs à l'autorité nationale compétente.

Dans le cadre du RSP, la notion de négligence grave implique plus que de la simple négligence et doit comporter un défaut de vigilance caractérisé, comme le fait de conserver les données de sécurité utilisées pour autoriser une opération de paiement à côté de l'instrument de paiement, sous une forme aisément accessible et reconnaissable par des tiers. Le fait qu'un e client e ait déjà reçu un remboursement d'une banque après avoir été victime d'une fraude par usurpation de l'identité d'un employé de banque et qu'il/elle introduise une autre demande de remboursement auprès de la même banque après avoir été à nouveau victime du même type de fraude pourrait être considéré comme une négligence grave : cela pourrait indiquer un niveau élevé d'imprudence de la part de cette personne qui aurait dû être plus vigilante après avoir déjà été victime du même mode opératoire frauduleux. Compte tenu des interprétations différentes de la notion de négligence grave au sein de l'UE, il est prévu que l'Autorité bancaire européenne publie des lignes directives afin de préciser les circonstances de fait qui devraient être prises en compte.

Avec le RSP, si chaque client e bancaire est tenu e de rester vigilant e, le paiement numérique devient aussi un écosystème de risques partagés entre banques, opérateurs télécoms, prestataires techniques, plateformes et utilisateur·rice·s.

En matière d'usurpation d'identité de la banque par les escrocs (nom de domaine, numéro de téléphone, adresse électronique, site web, application de la banque), le texte exige des banques la mise en place de mesures techniques robustes pour empêcher l'usurpation frauduleuse de leurs canaux de communication. Si une banque ne met pas en œuvre les mécanismes appropriés de prévention de la fraude, elle sera responsable de la couverture des pertes de ses client·e·s.

Les banques devront appliquer l'authentification forte à davantage d'opérations, quand leur client·e·s active une application mobile liée à leur compte, accèdent à leur compte en ligne, effectuent un ordre de paiement électronique, augmentent leurs plafonds, modifient un mot de passe ou leurs coordonnées, etc. Les exceptions au recours à l'authentification forte deviennent très limitées.

A cet égard, le texte prend également en compte la question de l'inclusion de l'ensemble de la clientèle : une authentification forte ne doit pas dépendre d'un seul appareil, d'une seule technologie ou d'un smartphone : les personnes handicapées, les personnes âgées, les personnes peu à l'aise avec le numérique et celles ne disposant pas d'un smartphone doivent avoir accès à des moyens adaptés.

Les banques doivent aussi proposer un service permettant de vérifier la concordance entre le nom du ou de la bénéficiaire et son identifiant unique/IBAN. Si le service de vérification ne fonctionne pas correctement ou si une divergence n'est pas signalée à la personne qui est en train d'effectuer le paiement, la banque sera tenue responsable du préjudice financier subi.

Une banque pourra suspendre ou refuser l'exécution d'un ordre de paiement lorsqu'il existe des motifs

objectivement justifiés de soupçonner une fraude.

Le RSP prévoit la possibilité pour les client·e·s bancaires de fixer des limites de montant maximal par instrument ou moyen de paiement, par transaction ou sur une période déterminée (un jour, une semaine par exemple). Toute augmentation à distance de ces limites peut être soumise à un délai de sécurité afin d'éviter qu'un escroc ne manipule sa victime pour relever immédiatement ses plafonds.

L'activation d'une application mobile sur un appareil doit passer par une authentification forte mais aussi par un délai d'activation afin de permettre à la victime d'intervenir si elle n'est pas à l'origine de l'activation. Le RSP parle d'un délai de quatre heures. La banque devra également informer chaque client e, de manière sécurisée et par différents canaux de communication, de l'activation d'une application mobile liée à son compte de paiement sur un appareil, s'il existe une relation client entre eux. Cette notification vise à accroître la vigilance de chaque client e et devrait lui permettre d'alerter sa banque s'il elle n'a pas installé l'application.

Le RSP élargit aussi la chaîne de responsabilité. Les fraudes aux paiements transitent le plus souvent par des appels téléphoniques, des emails, des sites web, des publicités frauduleuses ou des plateformes. Le texte prévoit des obligations et des mécanismes de coopération entre banques, opérateurs télécom, hébergeurs de sites, grandes plateformes en ligne et moteurs de recherche. Le RSP vise notamment la détection de l'usurpation d'identité, la lutte contre les publicités frauduleuses et l'échange d'informations.

Le RSP prévoit également la création d'une plateforme d'expert e s sur la lutte contre la fraude qui impliquerait autorités, banques, opérateurs télécoms, fournisseurs techniques, plateformes en ligne, commerçant e s, associations de consommateur rice s et organismes en charge du règlement des litiges. Cette plateforme permettra de partager les tendances, les pratiques, les menaces et les réponses. Le texte reconnaît que la fraude évolue plus vite que la législation. Si la législation fixe des obligations, il est aussi important de permettre une réaction rapide qui exige information, coopération, un système d'alertes rapides et une capacité d'adaptation permanente.

S'il est adopté en l'état, cette proposition de règlement devrait apporter une véritable amélioration de la situation des victimes de phishing. Un bémol toutefois : il nous semble que la banque ne devrait pas être juge de l'appréciation de la négligence grave de la part de la victime, même si le RSP conditionne le refus de remboursement à la production d'éléments justificatifs. Cela veut dire qu'en cas de contestation du refus de remboursement, ce sera toujours à la victime d'engager un recours.

Conclusions

Au printemps 2026, un panel de 75 citoyen·ne·s e tiré·e·s au sort et représentatif·ive·s de la population s'est réuni pendant trois weekends pour émettre des recommandations pour « une banque plus sûre, plus accessible et plus proche des citoyen ne s à l'ère du numérique ». Cette initiative de Belfius[23], la banque qui rappelons-le avait inscrit dans ses conditions générales que les victimes de phishing ne seraient remboursées qu'après enquête, a conduit à la production de vingt recommandations dont sept portant sur « Faire de la prévention de la fraude et de la protection des victimes la norme ». Cela montre bien que la question des arnaques bancaires constitue une priorité pour la population belge. La banque Belfius se prononcera sur le suivi de ces recommandations en 2027. Il n'est pas du tout certain que les propositions législatives actuellement sur le bureau de la Chambre des représentants soient adoptées. Quant au RSP, un vote en séance plénière du Parlement est prévu en décembre 2026 et le texte voté ne sera applicable que vingt et un mois après son entrée en vigueur (après publication

[23] G1000, *75 citoyens formulent des recommandations pour l'avenir du secteur bancaire*, 10/06/2026, https://www.g1000.org/fr/nouvelles/75-citoyens-formulent-des-recommandations-pour-lavenir-du-secteur-bancaire

au Journal officiel de l'UE).

En attendant, le ministre Beenders, en charge de la protection des consommateur·rice·s, qui serait en train de travailler sur une législation interprétative des dispositions du CDE relatives aux services de paiement, a lancé un appel public aux banques afin qu'elles élaborent un plan d'action pour lutter contre les fraudes bancaires. Le secteur bancaire a fait savoir qu'il intercepte 75% des virements générés par du phishing, qu'il a mis en place un numéro de téléphone général à contacter en cas de fraude grâce à l'extension du service Cardstop. Le secteur bancaire met en avant que la lutte contre la fraude n'est pas de sa seule responsabilité, mais constitue un problème sociétal et par conséquent une responsabilité partagée avec les entreprise de télécom et les plateformes de réseaux sociaux, mais aussi avec les pouvoirs publics[24].

Le ministre tente de faire pression sur les banques par différentes mesures. Dans un courrier qui leur a été adressé en avril dernier[25], il leur a demandés :

- de faire preuve d'une transparence totale quant aux critères utilisés pour établir la « négligence grave ». Elles doivent transmettre leurs check-lists internes et leurs cadres d'évaluation à son cabinet ;
- d'indiquer sur quelle base juridique elles s'appuient pour ne pas appliquer la procédure de remboursement prévue par la loi.

Entre-temps, les victimes passées du phishing ne récupéreront sans doute jamais l'argent qu'elles ont perdu. Nombre d'entre elles continueront aussi à vivre avec des blessures psychologiques (honte, stress, anxiété ou perte de confiance) provoquées par ces arnaques[26]. Compte tenu de la sophistication croissante des pratiques développées par les escrocs, d'autres victimes seront lésées avant que les différentes mesures annoncées ne produisent leurs effets.

Est-ce cela le prix à payer du passage à la banque numérique ?

[24] Febelfin, *La lutte contre le phishing est une responsabilité partagée*, 22/03/2026, https://febelfin.be/fr/presse/fraude-et-securite/la-lutte-contre-le-phishing-est-une-responsabilite-partagee-un-plan-d-action-commun-associant-les-operateurs-de-telecommunications-les-plateformes-de-reseaux-sociaux-et-les-pouvoirs-publics-s-impose

[25] Le ministre Beenders accentue la pression sur les banques : « Les clients ont le droit de savoir quand les banques les tiennent pour responsables en cas de phishing », CP 01/04/2026, https://beenders.belgium.be/fr/actualites/le-ministre-beenders-accentue-la-pression-sur-les-banques-les-clients-ont-le-droit-de

[26] Leray C. *Après une cyberarnaque, la santé mentale des victimes chamboulée : «La honte agit comme une seconde agression»*, Liberation, 06/04/2026, https://www.liberation.fr/societe/sante/la-honte-agit-comme-une-seconde-agression-apres-une-cyberarnaque-la-sante-mentale-des-victimes-chamboulee-20260406_34TPIIKN3RAHLI6M7AYMI75CRY/ (article réservé aux abonné e s)

Recommandations Financité

En lien avec cette analyse, le mémorandum Financité *« 52 propositions pour une finance au service de l'intérêt général, proche et adaptée aux citoyen·ne·s »* [27] plaide pour.

Les banques disposant du monopole des dépôts de par la loi, elles ont en contrepartie des obligations de service vis-à-vis de leur clientèle. Que l'on habite dans une commune pauvre ou riche, rurale ou urbaine, tout le monde devrait donc pouvoir accéder à un service bancaire de proximité qu'il faudrait inscrire dans la loi bancaire sur la base des principes suivants :

- une distance maximale à parcourir prenant en compte les différents moyens d'accès des personnes « non digitalisées » ;
- des solutions variées prenant en compte les besoins de la population : agence fixe, agence mobile, visites à domicile, etc ;
- des services bancaires par téléphone dans toutes les banques afin de pouvoir au minimum effectuer des virements et connaître la situation de son compte ;
- un véritable service téléphonique d'aide avec accès direct à des employé·e·s (et non un centre d'appels automatisé) spécialement formés à l'écoute, qui pourront répondre aux questions des personnes confrontées à des difficultés. Ces employé·e·s devraient disposer d'un temps raisonnable pour répondre aux questions.
- Prévoir des sanctions dissuasives contre les banques qui ne remboursent pas immédiatement leurs clients victimes de fraude qui n'ont commis aucune faute.
- Mise en place au niveau européen d'un contrôle nom-IBAN pour limiter les fraudes.

[27] Mémorandum Financité 2024 / https://www.financite.be/fr/news/decouvrez-notre-memorandum-en-vue-des-elections-2024

A propos de Financité

Si vous le souhaitez, vous pouvez nous contacter pour organiser avec votre groupe ou organisation une animation autour d'une ou plusieurs de ces analyses. Cette analyse s'intègre dans une des 5 thématiques traitées par Financité, à savoir :

Environnement : Nous pensons que la finance doit urgemment accompagner la transition écologique. La charge des investissements supplémentaires nécessaires ne pas porter atteinte à la satisfaction des besoins essentiels de la population et, en particulier, des classes populaires. Depuis 2005, nous analysons la qualité des produits d'investissement socialement responsable au travers de listes noires d'investissement et plaidons pour la mise en place d'une norme légale minimale stricte pour qualifier un fonds d'investissement de durable.

Inclusion : L'inclusion financière fait référence à un processus par lequel une personne peut accéder à et/ou utiliser des services et produits financiers proposés par des prestataires classiques, adaptés à ses besoins et lui permettant de mener une vie sociale normale. Financité a développé une activité importante en matière d'inclusion financière depuis le début des années 2000 : études sur l'élaboration d'un service bancaire universel, études sur l'inclusion financière, analyses, animations, plaidoyer… Elle a créé et participé au European Financial Inclusion Network (EFIN) et à divers programmes de microépargne et de prévention du surendettement.

Responsabilité : La finance peut être qualifiée de responsable si elle porte la même attention aux conséquences sociales, environnementales et économiques de son activité ou, pour le dire autrement, si elle ne porte pas atteinte à l'intérêt général. Pour s'assurer que la finance serve l'intérêt général, Financité s'intéresse notamment à la stabilité du secteur et aux deux grands facteurs de production, le capital et le travail. Nous y consacrons des analyses, animations, plaidoyer… mais nous approchons aussi cette dimension au travers de partenariats comme la Coalition Corona ou le Réseau pour la Justice fiscale.

Solidarité : La finance solidaire est une finance responsable plus engagée puisqu'elle consiste à fournir, sans visée spéculative et moyennant une rémunération limitée, l'argent nécessaire à la réalisation d'opérations économiques qui présentent une valeur ajoutée pour l'humain, la culture et/ou l'environnement, en vue de favoriser le bien commun, la cohésion sociale et la gouvernance démocratique. Pour promouvoir cette finance solidaire, Financité est notamment à l'origine du label Finance solidaire et de la coopérative de financement de l'économie sociale F'in Common.

Proximité : Une finance de proximité favorise la création de réseaux d'échanges locaux, resserre les liens entre producteur·rice·s et consommateur·rice·s et soutient financièrement les initiatives au niveau local. Notre objectif est de favoriser les filières de circuit courts et d'économie circulaire ainsi qu'une consommation responsable, notamment à travers la mise en place de systèmes d'échanges comme les monnaies locales et citoyennes.

Depuis 1987, des associations, des citoyen·ne·s et des acteurs sociaux se rassemblent au sein de Financité pour développer et promouvoir la finance responsable et solidaire.

L'ASBL Financité est reconnue par la Communauté française pour son travail d'éducation permanente.