DOC 56 **1592/001**

BELGISCHE KAMER VAN
VOLKSVERTEGENWOORDIGERS

2 juni 2026

WETSVOORSTEL

**tot wijziging
van het Wetboek van economisch recht
betreffende de bescherming van de betaler
bij niet-toegestane betalingstransacties
als gevolg van phishing**

(ingediend door de heer Jeroen Soete)

CHAMBRE DES REPRÉSENTANTS
DE BELGIQUE

2 juin 2026

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 de phishing**

(déposée par M. Jeroen Soete)

N-VA	:	*Nieuw-Vlaamse Alliantie*
VB	:	*Vlaams Belang*
MR	:	*Mouvement Réformateur*
PS	:	*Parti Socialiste*
PVDA-PTB	:	*Partij van de Arbeid van België – Parti du Travail de Belgique*
Les Engagés	:	*Les Engagés*
Vooruit	:	*Vooruit*
cd&v	:	*Christen-Democratisch en Vlaams*
Ecolo-Groen	:	*Ecologistes Confédérés pour l'organisation de luttes originales – Groen*
Anders.	:	*Anders.*
DéFI	:	*Démocrate Fédéraliste Indépendant*
ONAFH/INDÉP	:	*Onafhankelijk-Indépendant*

Afkorting bij de nummering van de publicaties:		*Abréviations dans la numérotation des publications:*	
DOC 56 0000/000	*Parlementair document van de 56e zittingsperiode + basisnummer en volgnummer*	*DOC 56 0000/000*	*Document de la 56e législature, suivi du numéro de base et numéro de suivi*
QRVA	*Schriftelijke Vragen en Antwoorden*	*QRVA*	*Questions et Réponses écrites*
CRIV	*Voorlopige versie van het Integraal Verslag*	*CRIV*	*Version provisoire du Compte Rendu Intégral*
CRABV	*Beknopt Verslag*	*CRABV*	*Compte Rendu Analytique*
CRIV	*Integraal Verslag, met links het definitieve integraal verslag en rechts het vertaalde beknopt verslag van de toespraken (met de bijlagen)*	*CRIV*	*Compte Rendu Intégral, avec, à gauche, le compte rendu intégral et, à droite, le compte rendu analytique traduit des interventions (avec les annexes)*
PLEN	*Plenum*	*PLEN*	*Séance plénière*
COM	*Commissievergadering*	*COM*	*Réunion de commission*
MOT	*Moties tot besluit van interpellaties (beigekleurig papier)*	*MOT*	*Motions déposées en conclusion d'interpellations (papier beige)*

SAMENVATTING

De digitalisering van de samenleving en het betalingsverkeer heeft geleid tot een sterke toename van phishing, dat vandaag een van de meest voorkomende vormen van criminaliteit in België is. Bijna de helft van de bevolking werd recent geconfronteerd met phishing, en ook succesvolle aanvallen treffen een aanzienlijke groep. De impact gaat verder dan financiële schade en veroorzaakt stress, onveiligheidsgevoelens en zelfs problemen bij het voorzien in basisbehoeften.

De financiële schade is enorm en België behoort zelfs tot de zwaarst getroffen landen in Europa. De kosten worden bovendien onevenredig gedragen door de consument. Bij phishingfraude betaalt het slachtoffer in België ongeveer 92 % van de schade zelf, wat sterk afwijkt van andere vormen van fraude waar banken meer verantwoordelijkheid dragen.

Het wetsvoorstel beoogt een aantal tekortkomingen in de huidige wetgeving aan te pakken. Zo wordt voorgesteld dat een betalingstransactie slechts als toegestaan kan worden aangemerkt indien de betaler zelf uitdrukkelijk heeft ingestemd met de uitvoering van de betalingsopdracht. Daarnaast moeten banken onmiddellijk terugbetalen, ook bij vermoedens van grove nalatigheid, met automatische interesten en mogelijke sancties als ze dit niet doen.

Tot slot worden strikte termijnen en transparantieverplichtingen voorgesteld, zodat slachtoffers snel een gemotiveerde beslissing krijgen en beter geïnformeerd worden over hun rechten.

RÉSUMÉ

La numérisation de la société et des opérations de paiement a entraîné une forte augmentation du phénomène de phishing (hameçonnage), qui constitue aujourd'hui l'une des formes de criminalité les plus courantes en Belgique. Près de la moitié de la population a été récemment confrontée au phishing, et les attaques réussies touchent, elles aussi, un nombre considérable de personnes. Ce phénomène a un impact qui va au-delà du préjudice financier; il génère du stress, un sentiment d'insécurité et même des difficultés à subvenir aux besoins de base.

Le préjudice financier est énorme et la Belgique figure même parmi les pays les plus touchés d'Europe. De plus, les coûts sont supportés de manière disproportionnée par le consommateur. En cas de fraude par phishing, la victime en Belgique paie elle-même environ 92 % du préjudice, soit un pourcentage bien plus élevé que pour d'autres formes de fraude, où les banques assument une plus grande responsabilité.

Cette proposition de loi vise à remédier à certaines lacunes de la législation actuelle. Il est ainsi proposé de faire en sorte qu'une opération de paiement ne puisse être considérée comme autorisée que si le payeur a lui-même consenti expressément à l'exécution de l'ordre de paiement. En outre, les banques doivent procéder à un remboursement immédiat, même en cas de suspicion de négligence grave, avec intérêts automatiques et sanctions éventuelles à la clé si elles ne le font pas.

Enfin, la proposition prévoit des délais stricts et des obligations de transparence, afin que les victimes reçoivent rapidement une décision motivée et soient mieux informées de leurs droits.

TOELICHTING

DAMES EN HEREN,

1. **Slachtoffers**

De digitalisering van onze maatschappij en ons betalingsverkeer heeft ontegensprekelijk vele voordelen met zich meegebracht, maar heeft tegelijkertijd de deuren wagenwijd opengezet voor nieuwe, massale vormen van criminaliteit. Waar vermogensdelicten jaren geleden nog hoofdzakelijk bestonden uit fysieke diefstal of het misbruik van cheques, is criminaliteit vandaag de dag gedigitaliseerd, geglobaliseerd en geprofessionaliseerd. Uit de recentste cijfers blijkt overduidelijk dat phishing is uitgegroeid tot het crimineel fenomeen waar de Belgische burger het vaakst mee geconfronteerd wordt.

Volgens de veiligheidsmonitor 2024 is bijna de helft van de bevolking (49,3 %) tussen 2023 en 2024 in aanraking gekomen met phishing, wat de meest significante toename is van alle onderzochte criminaliteitsfenomenen (komende van 40,1 % in 2021)[1]. Loutere pogingen tot phishing staan met 48,6 % op de absolute nummer één in de top 10 van criminaliteitsvormen waar burgers het slachtoffer van worden. Ook de voltooide phishingaanvallen (waarbij de fraudeurs in hun opzet slagen) treffen een aanzienlijke groep en staan op de vijfde plaats met 6,8 % van de bevolking als slachtoffer[2].

Deze criminaliteitsgolf laat bovendien diepe menselijke sporen na. De impact reikt veel verder dan enkel financiële schade. Van de slachtoffers van voltooide phishing geeft 17 % aan zich vaak of altijd onveilig te voelen[3]. 59 % van de slachtoffers voelt zich gestresseerd door de gebeurtenis en 41 % ervaart een aanzienlijke of matige impact op het algemene mentale welzijn. Bijna 1 op 10 slachtoffers gaf zelfs aan dat zij door de oplichting niet meer in staat waren om in hun basisbehoeften te voorzien[4].

2. **Dark number**

Wanneer we de verschillende nationale en internationale rapporten naast elkaar leggen, ontstaat er een

1 Federale politie (DRI/BIPOL), Federale analyse van de Veiligheidsmonitor 2024, Brussel, 2024, p. 38, *https://www.politie.be/statistieken/nl/veiligheidsmonitor*

2 Veiligheidsmonitor 2024, Federale Politie, 2024, blz. 36.

3 Veiligheidsmonitor 2024, Federale Politie, 2024, blz. 33.

4 State of Scams in Belgium 2025 Report, GASA, 2025, blz. 31-32.

DÉVELOPPEMENTS

MESDAMES, MESSIEURS,

1. **Victimes**

La numérisation de notre société et de nos opérations de paiement s'est indéniablement accompagnée de nombreux avantages, mais elle a, dans le même temps, ouvert grand la porte à de nouvelles formes de criminalité à grande échelle. Alors qu'il y a quelques années encore, les délits patrimoniaux consistaient principalement en des vols physiques ou en l'utilisation frauduleuse de chèques, la criminalité s'est aujourd'hui numérisée, mondialisée et professionnalisée. Les chiffres les plus récents montrent très clairement que le *phishing* est devenu le phénomène criminel auquel les citoyens belges sont le plus souvent confrontés.

Selon le Moniteur de sécurité 2024, près de la moitié de la population (49,3 %) – contre 40,1 % en 2021[1] – a été confrontée au *phishing* entre 2023 et 2024, ce qui constitue la hausse la plus marquante parmi tous les phénomènes criminels examinés. Avec une incidence de 48,6 %, les simples tentatives de *phishing* occupent, de loin, la première place dans le top 10 des formes de criminalité dont les citoyens sont victimes. Le *phishing* accompli (pratiques de *phishing* dont les auteurs parviennent à leurs fins) touche, lui aussi, un groupe important et arrive en cinquième position, 6,8 % de la population en étant victime[2].

Cette vague de criminalité laisse en outre de profondes traces sur le plan humain. Ses répercussions vont bien au-delà du simple préjudice financier. Parmi les victimes de *phishing* accompli, 17 % déclarent se sentir souvent ou toujours en insécurité[3]. 59 % des victimes se sentent stressées par cet événement et 41 % ressentent un impact important ou modéré sur leur bien-être mental général. Près d'une victime sur dix a même déclaré que l'escroquerie l'avait rendue incapable de subvenir à ses besoins fondamentaux[4].

2. **"Chiffre noir"**

La lecture comparée des différents rapports nationaux et internationaux fait apparaître un paradoxe inquiétant.

1 Police fédérale (DRI/BIPOL), Analyse fédérale du Moniteur de sécurité 2024, Bruxelles, 2024, p. 38, *https://www.police.be/statistiques/sites/statspol/files/statistics_files_upload/VMS%20Archive/11_VMS%202.024/VMS_2024_fr/01_F%C3%A9d%C3%A9ral/02_Tendances/Analyse_Moniteur_de_s%C3%A9curit%C3%A9_2024.pdf*

2 Moniteur de sécurité 2024, Police fédérale, 2024, p. 36.

3 Moniteur de sécurité 2024, Police fédérale, 2024, p. 33.

4 State of Scams in Belgium 2025 Report, GASA, 2025, p. 31-32.

verontrustende paradox. De schaal van de fraude is gigantisch, maar het bereikt de officiële handhavingskanalen nauwelijks.

Enerzijds zien we de miljoenen slachtoffers en de hallucinante cijfers van het Centrum voor Cybersecurity België (CCB) dat vorig jaar bijna 10 miljoen meldingen van verdachte berichten ontving via Safeonweb[5]. Anderzijds bereikt dit de politiediensten amper. De aangiftebereidheid bij de burger is vrijwel *nihil*: slechts 21 % van de slachtoffers van voltooide phishing en amper 4 % van de doelwitten van een poging stapt nog naar de politie[6].

Dit resulteert in een massaal dark number. De veiligheidsmonitor stelt letterlijk: "Hoewel internetfraude (phishing of andere) het meest gemelde feit is waarvan de respondenten slachtoffer waren in deze bevraging, is dit type criminaliteit, vanuit het oogpunt van de Politiële Criminaliteitsstatistieken (PCS), verre van proportioneel het meest geregistreerd. De cijfers in de PCS laten immers een geleidelijke toename van oplichting/internetfraude zien sinds meerdere jaren (bijna 10 keer meer geregistreerde feiten per jaar in 13 jaar, van 4312 geregistreerde feiten in 2011 tot 41.291 in 2023). Bovendien was er tussen 2018 en 2022 een duidelijke stijging van de registraties, maar een lichte daling tussen 2022 en 2023 (-2 %). De vergelijking van de PCS (officieel geregistreerde criminaliteit) en de resultaten van de Veiligheidsmonitor (zelfgerapporteerd slachtofferschap) in relatie tot verschillende fenomenen stelt ons in staat om een zeer groot dark number te vermoeden in het domein van oplichting/internetfraude, en zeker een van de belangrijkste, zo niet HET belangrijkste.[7]"

3. **Financiële schade**

Hoewel we door de lage aangiftebereidheid slechts het topje van de ijsberg zien, is de economische schade die door de mazen van het net glipt nu al astronomisch. De financiële impact van dit fenomeen is catastrofaal en België wordt hierbij onevenredig hard geraakt in vergelijking met de rest van Europa.

Het rapport van de Europese Bankautoriteit (EBA) en de Europese Centrale Bank (ECB) toont aan dat in België

5 Centrum voor Cybersecurity België (CCB), Kerncijfers 2025, Brussel, 2025, *https://ccb.belgium.be/nl/news/kerncijfers-2025*

6 Veiligheidsmonitor 2024, Federale Politie, 2024, blz. 47.

7 Veiligheidsmonitor 2024, Federale Politie, 2024, blz. 37.

L'ampleur de la fraude est gigantesque, mais les faits ne sont qu'à peine relayés auprès des canaux officiels de lutte contre la criminalité.

D'une part, on constate des millions de victimes et il y a les chiffres hallucinants du Centre pour la Cybersécurité Belgique (CCB), qui a reçu l'année dernière, via la plateforme Safeonweb, près de 10 millions de signalements de messages suspects[5]. D'autre part, les faits en question ne bénéficient guère d'un écho auprès des services de police. La propension des citoyens à déclarer les faits est très faible: 21 % seulement des victimes de *phishing* accompli et à peine 4 % des cibles d'une tentative contactent à la police[6].

Il en résulte un très grand nombre de cas non recensés ("chiffre noir"), comme on peut le lire dans le Moniteur de sécurité: "Alors que les escroqueries via Internet (*phishing* ou autres) sont les faits dont les répondants rapportent le plus largement avoir été victimes dans la présente enquête, du point de vue des statistiques policières de criminalité (SPC), ce type de criminalité est bien loin d'être proportionnellement le plus enregistré. Les chiffres des SPC montrent une augmentation progressive des escroqueries/fraudes via Internet depuis plusieurs années (près de 10 fois plus de faits enregistrés par an en 13 ans, passant de 4312 faits enregistrés en 2011 à 41.291 en 2023). De plus, alors qu'on remarquait une nette augmentation des enregistrements entre 2018 et 2022, on note une légère diminution des chiffres entre 2022 et 2023 (-2 %). La mise en parallèle des SPC (criminalité officielle enregistrée) et des résultats du Moniteur de sécurité (victimisation auto-rapportée) par rapport à divers phénomènes nous permet de soupçonner un chiffre noir très important en matière d'escroqueries/de fraudes sur Internet, chiffre noir certainement parmi les plus importants, si ce n'est LE plus important.[7]"

3. **Préjudice financier**

Vu la faible propension à déclarer les faits, seule la partie émergée de l'iceberg est visible, mais le préjudice économique est en réalité astronomique en raison de la fraude qui passe entre les mailles du filet. Ce phénomène a des conséquences financières catastrophiques et la Belgique est proportionnellement parlant plus durement touchée que le reste de l'Europe.

Le rapport de l'Autorité bancaire européenne (ABE) et de la Banque centrale européenne (BCE) montre

5 Centre pour la Cybersécurité Belgique (CCB), Chiffres clés 2025, Bruxelles, 2025, *https://ccb.belgium.be/fr/news/chiffres-cles-2025*

6 Moniteur de sécurité 2024, Police fédérale, 2024, p. 47.

7 Moniteur de sécurité 2024, Police fédérale, 2024, p. 37.

in 2024 via alle vormen van betalingsfraude 272 miljoen euro werd gestolen[8]. Wanneer we inzoomen op fraude met overschrijvingen (in de praktijk voor 74 %[9] het directe gevolg van phishing) zien we dat er in België maar liefst 216 miljoen werd weggesluisd.

De Europese vergelijking is pijnlijk, hoewel België qua bevolkingsomvang verre van het grootste land is, bekleden we wat betreft de absolute financiële schade door frauduleuze overschrijvingen de trieste derde plaats in Europa. Met een verlies van 216 miljoen euro moeten we enkel Duitsland (474 miljoen) en Frankrijk (350 miljoen) laten voorgaan. Landen met een veel grotere bevolking, zoals Italië en Polen, lijden aanzienlijk minder schade[10].

Deze torenhoge financiële schade vertaalt zich in een hallucinant aantal individuele drama's op dagelijkse basis. Uit ditzelfde Europese rapport blijkt immers dat er in België in 2024 maar liefst 87.235 frauduleuze overschrijvingen werden uitgevoerd[11]. Dit betekent onomwonden dat er in ons land gemiddeld 239 keer per dag een frauduleuze overschrijving succesvol wordt voltooid door criminelen. De gemiddelde schade per frauduleuze overschrijving bedraagt in België bijna 2500 euro[12].

Deze geregistreerde bankcijfers tonen bovendien slechts een deel van de werkelijkheid. Febelfin meldt dat de banksector in 2024 erin slaagde om 75 % van de frauduleuze overschrijvingen als gevolg van phishing te detecteren, tegen te houden of terug te vorderen. Ondanks dit hoge detectiepercentage bleken fraudeurs in 2024 via de resterende 25 % alsnog 49 miljoen euro buit te maken in België[13][14].

Deze trend zet zich bovendien fors door. Januari en februari 2026 blijken absolute "topmaanden" te zijn, waarbij de fraudecijfers nog hoger liggen dan in dezelfde periode vorig jaar. In het gerechtelijke arrondissement

8 European Banking Authority (EBA) & European Central Bank (ECB), 2025 Report on Payment Fraud, 2025, *https://www.ecb.europa.eu/press/intro/publications/pdf/ecb.ebaecb202512.en.pdf,* blz. 45.

9 2025 Report on Payment Fraud, EBA&ECB, 2025, blz. 19.

10 2025 Report on Payment Fraud, EBA&ECB, 2025.

11 2025 Report on Payment Fraud, EBA&ECB, 2025, blz. 45.

12 2025 Report on Payment Fraud, EBA&ECB, 2025, blz. 44-45.

13 Belgische Federatie van de financiële sector (FEBELFIN), If it smells phishy, it probably is!, 2025, *https://febelfin.be/en/press-room/fraude-veiligheid/if-it-smells-phishy-it-probably-is,* blz. 2.

14 GASA raamt de totale schade door alle vormen van scams en oplichting in België op 4,2 miljard euro in het afgelopen jaar. (State of Scams in Belgium 2025 Report, blz. 5).

que le montant dérobé par le biais de l'ensemble des formes de fraude aux paiements s'élevait en Belgique, en 2024, à 272 millions d'euros[8]. Si l'on examine plus particulièrement la fraude par virement (qui est, en pratique, dans 74 %[9] des cas, la conséquence directe du *phishing*), on voit que le montant volé en Belgique par cette voie atteignait pas moins de 216 millions d'euros.

La comparaison européenne est douloureuse: loin d'être le pays le plus important en termes de chiffre de population, la Belgique n'en occupe pas moins la triste troisième place en Europe en ce qui concerne le préjudice financier absolu résultant de virements frauduleux. Avec une perte de 216 millions d'euros, elle est seulement devancée par l'Allemagne (474 millions) et la France (350 millions). Des pays nettement plus peuplés, comme l'Italie et la Pologne, subissent des pertes beaucoup moins importantes[10].

Ces pertes financières colossales se traduisent par un nombre ahurissant de drames individuels sur une base journalière. Ce même rapport européen révèle en effet qu'en Belgique, pas moins de 87.235 virements frauduleux ont été effectués en 2024[11]. Cela signifie clairement que, chaque jour, dans notre pays, 239 virements frauduleux sont effectués avec succès par des criminels. Le préjudice moyen par virement frauduleux s'élève en Belgique à près de 2500 euros[12].

Ces chiffres bancaires enregistrés ne reflètent de surcroît qu'une partie de la réalité. Febelfin indique qu'en 2024, le secteur bancaire a réussi à détecter, bloquer ou récupérer 75 % des virements frauduleux résultant du *phishing*. En dépit de ce taux de détection élevé, les fraudeurs sont quand même parvenus, par les 25 % de virements restants, à détourner 49 millions d'euros en Belgique en 2024[13][14].

Et cette tendance est loin de s'affaiblir. Les mois de janvier et février 2026 apparaissent d'ailleurs comme des "mois de records" absolus, avec des chiffres de fraude encore plus élevés que ceux enregistrés l'année dernière

8 Autorité bancaire européenne (ABE) & Banque centrale européenne (BCE), 2025 Report on Payment Fraud, 2025, *https://www.ecb.europa.eu/press/intro/publications/pdf/ecb.ebaecb202512.en.pdf,* p. 45.

9 2025 Report on Payment Fraud, EBA&ECB, 2025, p. 19.

10 2025 Report on Payment Fraud, EBA&ECB, 2025.

11 2025 Report on Payment Fraud, EBA&ECB, 2025, p 45.

12 2025 Report on Payment Fraud, EBA&ECB, 2025, p 44-45.

13 Fédération belge du secteur financier (FEBELFIN), Si ça ressemble à du phishing, c'est probablement du phishing!, 2025, *https://https://febelfin.be/fr/presse/fraude-et-securite/si-ca-ressemble-a-du-phishing-c-est-probablement-du-phishing,* p. 2.

14 GASA évalue le montant total des dommages causés par toutes les formes d'arnaques et d'escroqueries en Belgique à 4,2 milliards d'euros pour l'année écoulée (*State of Scams in Belgium 2025 Report*, p. 5).

Antwerpen staat de teller momenteel al op bijna 10 miljoen euro schade en 800 nieuwe dossiers, louter en alleen voor phishing[15]. We kijken bij een voorzichtige raming minstens aan tegen een verdrievoudiging van het schadebedrag aan phishing ten opzichte van 2024.[16]

4. **Consument betaalt de prijs**

De kern van het huidige probleem ligt niet alleen in de hoogte van de bedragen, maar in de manier waarop deze schade wordt verdeeld. Er is sprake van een schokkende asymmetrie tussen de bescherming bij fysieke diefstal en de bescherming bij digitale oplichting. Ondanks de massale schaal en geraffineerde technieken van cybercriminelen, draait het slachtoffer vrijwel volledig zelf op voor de kosten.

Volgens cijfers van de ECB wordt bij frauduleuze overschrijvingen de schade in België maar liefst 92 % gedragen door de consument, en niet door de bank[17]. Dit ligt nog aanzienlijk hoger dan het Europese gemiddelde van 85 %. In het merendeel van de gevallen blijft de consument dus met lege handen achter.

Deze situatie is uiterst scheef wanneer we ze vergelijken met andere vormen van betalingsfraude. Bij klassieke kaartfraude (waarbij men in 2024 ruim 53 miljoen euro buit maakte in België) zijn de verliezen veel evenwichtiger verdeeld: de Belgische consument draagt hier 54 % van het verlies. Bij fraude met domiciliëringen dragen de Belgische banken zelf 100 % van het verlies[18].

Phishing is in wezen niets anders dan de diefstal van een “digitale kaart” of “digitale sleutel” van de consument. Toch wordt het slachtoffer van phishing door de huidige interpretatie van de wetgeving en bankvoorwaarden aanzienlijk slechter beschermd dan het slachtoffer van een fysieke kaartdiefstal.

5. **Maatschappelijke verontwaardiging**

Wanneer de consument, zoals in het vorig punt aangetoond, vrijwel uitsluitend opdraait voor deze financiële

[15] Phishing, drugs en bendes: criminaliteit in cijfers", *vrt.be*, 27 februari 2026, *https://www.vrt.be/vrtnws/nl/2026/02/27/phishing-drugs-bendes-criminaliteit-cijfers-geweld/*

[16] Bij extrapolatie Antwerpse cijfers van 2025 naar Vlaanderen: ongeveer 150 miljoen euro. Bij extrapolatie Antwerpse cijfers (jan/feb 2026): ongeveer 200 miljoen euro.

[17] 2025 Report on Payment Fraud, EBA&ECB, 2025, blz. 37.

[18] 2025 Report on Payment Fraud, EBA&ECB, 2025, blz. 36.

à la même période. Dans l’arrondissement judiciaire d’Anvers, on compte déjà près de 10 millions d’euros de préjudice et 800 nouveaux dossiers, rien que pour le *phishing*[15]. Une estimation prudente table sur un triplement au minimum du montant du préjudice résultant du *phishing* par rapport au montant de 2024.[16]

4. **Le consommateur paie le prix**

Le nœud du problème actuel tient non seulement à l’ampleur des montants en jeu, mais aussi à la répartition des coûts du préjudice. Il y a une asymétrie choquante entre la protection offerte en cas de vol physique et la protection offerte en cas d’escroquerie numérique. En dépit de l’ampleur du phénomène et des techniques sophistiquées des cybercriminels, c’est la victime elle-même qui supporte la quasi-totalité des coûts.

Selon les chiffres de la BCE, le préjudice résultant de virements frauduleux en Belgique est supporté non pas par la banque mais par le consommateur et dans une proportion de pas moins de 92 %[17], soit un pourcentage bien supérieur à la moyenne européenne qui est de 85 %. Dans la majorité des cas, le consommateur se retrouve donc les mains vides.

La situation est totalement différente lorsqu’il s’agit d’autres formes de fraude aux paiements. En cas de fraude classique à la carte (qui a causé un préjudice de plus de 53 millions d’euros en Belgique en 2024), les pertes sont réparties de manière beaucoup plus équilibrée: elles sont imputées au consommateur à hauteur de 54 %. En cas de fraude aux domiciliations, les banques belges supportent elles-mêmes 100 % de la perte[18].

Le *phishing* n’est rien d’autre en soi que le vol d’une “carte numérique” ou d’une “clé numérique” du consommateur. Or, en raison de l’interprétation actuelle de la législation et des conditions bancaires, la victime d’un *phishing* est nettement moins bien protégée que la victime d’un vol de carte physique.

5. **Indignation sociétale**

Lorsque le consommateur doit faire face seul ou presque à ce désastre financier, comme on l’a montré au

[15] Phishing, drugs en bendes: criminaliteit in cijfers", *vrt.be*, 27 février 2026, *https://www.vrt.be/vrtnws/nl/2026/02/27/phishing-drugs-bendes-criminaliteit-cijfers-geweld/*

[16] Si l’on extrapole les chiffres de 2025 relatifs à Anvers à la Flandre, on obtient un montant de près de 150 millions d’euros. Et si l’on extrapole les chiffres de janvier/février 2026 relatifs à Anvers, alors le montant grimpe à quelque 200 millions d’euros.

[17] 2025 Report on Payment Fraud, EBA&ECB, 2025, p. 37.

[18] 2025 Report on Payment Fraud, EBA&ECB, 2025, p. 36.

ravage, leidt dit onvermijdelijk tot zware persoonlijke drama's en een groeiende publieke verontwaardiging.

De schaal van het probleem en de schrijnende verhalen van gedupeerden leiden tot een breed maatschappelijk ongenoegen. Ombudsfin stelt expliciet vast dat er nooit eerder in de media zoveel aandacht werd besteed aan internetfraude als in de laatste jaren[19]. De frequente berichtgeving in de nationale media zoals *Het Laatste Nieuws, De Standaard, Het Nieuwsblad, de VRT,* enz. wijst op een maatschappelijk probleem dat onbeheersbaar wordt. Mainstream media, waaronder consumentenprogramma's zoals WinWin op Radio 2, wijden hele thema-uitzendingen aan de vloedgolf van klachten en vragen van wanhope luisteraars[20].

De publieke verontwaardiging richt zich hierbij steeds vaker op de houding van de financiële sector. In de pers verschijnen aan de lopende band artikelen die de David-tegen-Goliath strijd tussen het slachtoffer en de bank illustreren[21].

Slachtoffers die, nadat hun rekening is geplunderd, bij hun vertrouwde bank aankloppen voor de wettelijk voorziene bescherming, botsten op een muur van onbegrip. Terwijl zij jarenlang moeten wachten op eventuele compensatie via de rechtbank, worden zij door hun financiële instelling vaak als schuldige afgedaan wegens een vermeende "toegelaten transactie" of "grove nalatigheid". Deze gang van zaken voedt niet alleen de maatschappelijke verontwaardiging, maar tast ook

19 Ombudsfin, Jaarverslag 2022, Brussel, 2022, blz. 17.

20 Experiment 'WinWin' over online oplichting: 13 van de 18 mensen gaven hun bankcodes aan een wildvreemde", *vrt.be*, 3 september 2025, *https://www.vrt.be/vrtnws/nl/2025/09/03/winwin-experiment-oplichting-13-van-de-18-mensen-gaven-hun-bank/*

21 — HLN, "Van ex-bankier tot IT'er, niemand lijkt nog veilig voor phishingbendes: "Plots stond er nog maar 26 cent op de rekening", 21 maart 2026.
— De Standaard, "Elke 2,5 seconden nieuwe melding van phishing: "Vroeger betaalden de banken slachtoffers terug, nu is er altijd discussie", 27 februari 2026.
— HLN: "Nieuw wapen in de strijd tegen phishingplaag: tool waarschuwt meteen voor oplichters", 18 maart 2026.
— HBVL: "Volgens de wet moeten banken slachtoffers van phishing vergoeden, maar dat gebeurt zelden: hoe komt dat?", 14 maart 2026.
— HLN, "Hij zei: "Je zal alles terugkrijgen, tot de laatste euro!" Maar toen was alles weg": Jacques (82) raakt 57.000 euro kwijt aan oplichters", 1 februari 2026.
— VRT NWS, "Phishing is een massaplaag: "Banken maken er een eigen-schuld-dikke-bultverhaal van", 5 maart 2026.
— GvA, "Bank moet slachtoffer van phishing terugbetalen, beslist rechter", 12 maart 2026.

point précédent, il est inévitable que de graves drames personnels surviennent et que l'indignation gagne la société.

L'ampleur du problème et les récits poignants des victimes provoquent un large mécontentement au sein de la société. Ombudsfin constate explicitement que la fraude sur Internet n'a jamais suscité autant d'attention médiatique que ces dernières années.[19] Les nombreuses informations relayées par les médias nationaux tels que *Het Laatste Nieuws*, *De Standaard*, *Het Nieuwsblad*, la VRT, etc. sont la preuve qu'il s'agit d'un problème sociétal hors de contrôle. Les médias traditionnels, avec, notamment, les programmes axés sur la défense des consommateurs comme *WinWin* sur Radio 2, consacrent des émissions thématiques entières à la vague de plaintes et de questions émanant d'auditeurs désespérés.[20]

C'est l'attitude du secteur financier qui tend à susciter de plus en plus l'indignation au sein de la société. La presse regorge d'articles montrant que ce genre d'affaire tourne vite, entre la victime et la banque, à un combat de David contre Goliath[21].

Les victimes qui, après avoir constaté que leur compte avait été vidé, se sont tournées vers leur banque habituelle pour bénéficier de la protection prévue par la loi, se sont heurtées à un mur d'incompréhension. Alors qu'elles doivent attendre des années avant d'obtenir éventuellement réparation par la voie judiciaire, les victimes sont souvent considérées comme responsables par leur établissement financier en raison d'une prétendue "opération autorisée" ou d'une "négligence grave".

19 Ombudsfin, Rapport annuel 2022, Bruxelles, 2022, p. 16.

20 "Experiment 'WinWin' over online oplichting: 13 van de 18 mensen gaven hun bankcodes aan een wildvreemde", *vrt.be*, 3 septembre 2025, *https://www.vrt.be/vrtnws/nl/2025/09/03/winwin-experiment-oplichting-13-van-de-18-mensen-gaven-hun-bank/*

21 — HLN, "Van ex-bankier tot IT'er, niemand lijkt nog veilig voor phishingbendes: "Plots stond er nog maar 26 cent op de rekening", 21 mars 2026.
— De Standaard, «Elke 2,5 seconden nieuwe melding van phishing: "Vroeger betaalden de banken slachtoffers terug, nu is er altijd discussie", 27 février 2026.
— HLN: "Nieuw wapen in de strijd tegen phishingplaag: tool waarschuwt meteen voor oplichters", 18 mars 2026.
— HBVL: "Volgens de wet moeten banken slachtoffers van phishing vergoeden, maar dat gebeurt zelden: hoe komt dat?", 14 mars 2026.
— HLN, «Hij zei: "Je zal alles terugkrijgen, tot de laatste euro!" Maar toen was alles weg": Jacques (82) raakt 57.000 euro kwijt aan oplichters", 1er février 2026.
— VRT NWS, «Phishing is een massaplaag: «Banken maken er een eigen-schuld-dikke-bultverhaal van», 5 mars 2026.
— GvA, «Bank moet slachtoffer van phishing terugbetalen, beslist rechter», 12 mars 2026.

het vertrouwen van de burger in het veilige gebruik van digitale betalingsdiensten aan[22].

6. **Tekortkomingen in de huidige wetgeving**

De huidige regels inzake betalingsdiensten, die voortvloeien uit de omzetting van de Europese PSD2-richtlijn in Boek VII van het Wetboek van economisch recht (WER), zijn in essentie ontworpen voor een tijdperk waarin fraude voornamelijk bestond uit het fysieke verlies of de diefstal van een bankkaart. Deze wetgeving is niet opgewassen tegen de moderne, uiterst geraffineerde vormen van social engineering en phishing waarmee de burger vandaag wordt geconfronteerd. De toepassing van deze verouderde regels in de praktijk laat de consument op meerdere vlakken in de kou staan. Op volgende cruciale punten schiet de huidige wetgeving tekort:

6.1. ***Toegestane vs. niet-toegestane betalingstransacties***

Twee Europese betalingsdienstrichtlijnen (beter bekend als PSD1[23] en PSD2[24]) beogen de betaler te beschermen tegen betaalfraude. De bepalingen uit deze richtlijnen zijn omgezet in Boek VII van het Wetboek van economisch recht.

Een cruciaal element binnen de fraudebeschermingsregeling is het onderscheid tussen toegestane en niet-toegestane betalingstransacties, aangezien de aansprakelijkheidsregels van de artikelen VII.43 en 44 WER uitsluitend van toepassing zijn bij niet-toegestane betalingstransacties. Bij betaalfraude dient men dan ook in eerste instantie dit onderscheid te maken.

Cette situation alimente non seulement l'indignation de la société, mais sape aussi la confiance du citoyen dans la sécurité des services de paiement numériques[22].

6. **Carences de la législation actuelle**

Les règles actuelles en matière de services de paiement, qui découlent de la transposition de la directive européenne sur les services de paiement 2015/2366 (DSP2) dans le Livre VII du Code de droit économique (CDE), ont été essentiellement conçues pour une époque où la fraude consistait principalement en la perte matérielle ou le vol d'une carte bancaire. Cette législation ne répond pas adéquatement aux formes modernes et extrêmement sophistiquées d'ingénierie sociale et de *phishing* auxquelles le citoyen est actuellement confronté. Dans la pratique, l'application de ces règles devenues obsolètes laisse le consommateur insuffisamment protégé à plusieurs égards. La législation actuelle s'avère insuffisante sur les points clés suivants:

6.1. ***Opérations de paiement autorisées ou non autorisées***

Deux directives européennes relatives aux services de paiement (DSP1[23] et DSP2[24]) visent à protéger le payeur contre la fraude en matière de paiements. Les dispositions de ces directives ont été transposées dans le Livre VII du Code de droit économique.

Un élément fondamental du dispositif de protection contre la fraude réside dans la distinction opérée entre les opérations de paiement autorisées et celles non autorisées, dans la mesure où les règles de responsabilité prévues aux articles VII.43 et VII.44 du CDE ne s'appliquent qu'aux opérations de paiement non autorisées. Dès lors, en cas de fraude en matière de paiements, il convient avant tout d'opérer cette distinction.

---

22 15.000 euro kwijt door phishing: beste banken, hoe kan het dat ons geld niet veilig is op onze rekeningen?", *Knack.be*, 19 november 2023, *https://www.knack.be/nieuws/belgie/justitie-belgie-belgisch-recht-rechtszaken-hervorming-justitie/15-000-euro-kwijt-door-phishing-beste-banken-hoe-kan-het-dat-ons-geld-niet-veilig-is-op-onze-rekeningen/*

23 Richtlijn 2007/64/EG van het Europees Parlement en de Raad van 13 november 2007 betreffende betalingsdiensten in de interne markt tot wijziging van de Richtlijnen 97/7/EG, 2002/65/EG, 2005/60/EG en 2006/48/EG, en tot intrekking van Richtlijn 97/5/EG.

24 Richtlijn (EU) 2015/2366 van het Europees Parlement en de Raad van 25 november 2015 betreffende betalingsdiensten in de interne markt, houdende wijziging van de Richtlijnen 2002/65/EG, 2009/110/EG en 2013/36/EU en Verordening (EU) nr. 1093/2010 en houdende intrekking van Richtlijn 2007/64/EG.

22 15.000 euro kwijt door phishing: beste banken, hoe kan het dat ons geld niet veilig is op onze rekeningen?", *Knack.be*, 19 novembre 2023, *https://www.knack.be/nieuws/belgie/justitie-belgie-belgisch-recht-rechtszaken-hervorming-justitie/15-000-euro-kwijt-door-phishing-beste-banken-hoe-kan-het-dat-ons-geld-niet-veilig-is-op-onze-rekeningen/*

23 Directive 2007/64/CE du Parlement européen et du Conseil du 13 novembre 2007 concernant les services de paiement dans le marché intérieur, modifiant les directives 97/7/CE, 2002/65/CE, 2005/60/CE ainsi que 2006/48/CE et abrogeant la directive 97/5/CE.

24 Directive (UE) 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur, modifiant les directives 2002/65/CE, 2009/110/CE et 2013/36/UE et le règlement (UE) n° 1093/2010, et abrogeant la directive 2007/64/CE.

De wet definieert beide begrippen als volgt:

— een betalingstransactie is toegestaan wanneer de betaler uitdrukkelijk heeft ingestemd met de uitvoering van de betalingsopdracht (art VII.32, § 1, WER);

— een betalingstransactie is niet toegestaan wanneer de betaler niet heeft ingestemd met de uitvoering ervan (art. VII.32, § 2, derde lid, WER).

De instemming dient te worden verleend in de tussen de betaler en de betalingsdienstaanbieder overeengekomen vorm en volgens de overeengekomen procedure (art. VII.32, § 2, eerste lid, WER).

Wanneer een betaler betwist een transactie te hebben toegestaan, kan de betalingsaanbieder hiertegenover stellen dat de transactie werd "geauthenticeerd", correct geregistreerd en niet door een technische storing beïnvloed (art. VII.42, § 1, WER *j.* artikel 59 PSD1).

Artikel I.9, 11° WER omschrijft authenticatie als "een procedure waarmee een betalingsdienstaanbieder de identiteit van een betalingsdienstgebruiker dan wel de validiteit van het gebruik van een specifiek betaalinstrument kan verifiëren, het gebruik van de persoonlijke beveiligingsgegevens van de betalingsdienstgebruiker inbegrepen". De betalingsdienstaanbieder moet met andere woorden bewijzen dat de contractuele voorwaarden rond betalingstransacties werden nageleefd. Als de betalingsdienstaanbieder hier niet in slaagt, dan gaat het om een niet-toegestane betalingstransactie en kan de betaler niet aansprakelijk worden gesteld.

In de praktijk rijst de vraag wat het bewijs van authenticatie impliceert wanneer de betalingsdienstaanbieder wél kan bewijzen dat de transactie in kwestie geauthenticeerd en correct geregistreerd werd. Sommige betalingsdienstaanbieders hanteren het standpunt dat bewezen authenticatie gelijkstaat aan instemming van de betaler, en het dus om een toegestane transactie gaat. Op die manier trachten betalingsdienstaanbieders te ontsnappen aan de toepassing van het aansprakelijkheidsregime voor niet-toegestane betalingstransacties.[25] Ombudsfin stelt echter dat een "dergelijke invulling van de wet waarbij autorisatie compleet gelijkstaat aan authenticatie" de bescherming die de Europese en Belgische wetgever aan de betaler wilde bieden nagenoeg volledig uitholt.[26] Het Hof van Justitie heeft deze visie van Ombudsfin bevestigd in het arrest *Eurobank Bulgaria*: zelfs indien de

[25] K. Dobbelaere, "Aansprakelijkheid bij phishing-fraude. Analyse van Belgische rechtspraak, met focus op het verhogen van de rechtszekerheid," thesis UGent, 2023-2024, 14-15.

[26] Ombudsfin, Jaarverslag 2022, 20.

La loi définit ces deux notions comme suit:

— une opération de paiement est autorisée lorsque le payeur a explicitement donné son consentement à l'exécution de l'ordre de paiement (art. VII.32, § 1er, CDE);

— une opération de paiement n'est pas autorisée lorsque le payeur n'a pas donné son consentement à son exécution (art. VII.32, § 2, alinéa 3, CDE).

Le consentement doit être donné sous la forme convenue entre le payeur et le prestataire de services de paiement et conformément à la procédure convenue (art. VII.32, § 2, alinéa 1er, CDE).

Lorsqu'un payeur nie avoir autorisé une opération de paiement, le prestataire de services de paiement peut objecter que l'opération a été "authentifiée", qu'elle a été correctement enregistrée et non affectée par une déficience technique (article VII.42, § 1er, du CDE, lu conjointement avec l'article 59 de la DSP1).

L'article I.9, 11°, du CDE définit l'authentification comme "une procédure permettant au prestataire de services de paiement de vérifier l'identité d'un utilisateur de services de paiement ou la validité de l'utilisation d'un instrument de paiement spécifique, y compris l'utilisation des données de sécurité personnalisées de l'utilisateur de services de paiement". En d'autres termes, le prestataire de services de paiement doit prouver que les conditions contractuelles encadrant les opérations de paiement ont été respectées. Si le prestataire de services de paiement ne parvient pas à rapporter cette preuve, il s'agit d'une opération de paiement non autorisée et la responsabilité du payeur ne peut être invoquée.

Dans la pratique, la question se pose de savoir ce qu'implique la preuve de l'authentification lorsque le prestataire de services de paiement parvient à prouver que ladite opération a été authentifiée et qu'elle a été correctement enregistrée. Certains prestataires de services de paiement considèrent qu'une authentification dûment établie équivaut au consentement du payeur et qu'il s'agit dès lors d'une opération autorisée. Ils cherchent ainsi à se soustraire à la mise en œuvre du régime de responsabilité applicable aux opérations de paiement non autorisées.[25] Mais selon Ombudsfin, "une telle interprétation de la loi, dans laquelle l'autorisation serait pleinement équivalente à l'authentification, éroderait presque totalement la protection que les législateurs européens et belges ont voulu offrir au payeur".[26] La Cour de justice a confirmé cette interprétation d'Ombudsfin

[25] K. Dobbelaere, "Aansprakelijkheid bij phishing-fraude. Analyse van Belgische rechtspraak, met focus op het verhogen van de rechtszekerheid", thèse Université de Gand, 2023-2024, 14-15.

[26] Ombudsfin, Rapport annuel 2022, 20.

overeengekomen authenticatieprocedure werd gevolgd, kan de transactie nog steeds niet-toegestaan zijn.[27]

Het is immers mogelijk dat de authenticatie het gebruik van het betaalinstrument met bijbehorende code bevestigt, doch dat het niet de betaler is die het instrument heeft gebruikt (en het aldus niet de betaler zelf is die instemming heeft verleend).

Meer concreet, wanneer iemand het slachtoffer is geworden van phishing en persoonlijke beveiligingsgegevens (bijvoorbeeld het kaartnummer, de vervaldatum en responscode/OTP) rechtstreeks (bijvoorbeeld via de telefoon) of onrechtstreeks (door deze in te voeren op een website waar naar hij via een hyperlink in een email of sms werd geleid) heeft gecommuniceerd aan de fraudeur gaat het om een niet-toegestane betalingstransactie. De betaler heeft alsdan niet zelf zijn instemming gegeven met de uitvoering van de betalingsopdracht. Hij heeft niet de opdracht verleend om een welbepaald bedrag op een welbepaalde rekening (hetgeen de essentie is van een betaalopdracht) over te maken. Enkel werden hem/haar (bijvoorbeeld telefonisch of online) gegevens ontfutseld die toelaten om een niet-toegestane betalingstransactie te initiëren of een betaalapplicatie te installeren.

Tevens bestond er onduidelijkheid over wie in dat geval de bewijslast draagt.[28] Ook dit werd door het Hof van Justitie beslecht: de bewijslast rust op de betalingsdienstaanbieder. Die moet aantonen dat de gebruiker in de overeengekomen vorm heeft ingestemd. Het enkele gebruik van een betaalinstrument volstaat daarvoor niet.[29]

dans l'arrêt *Eurobank Bulgaria*: même lorsque la procédure d'authentification convenue a été suivie, l'opération peut toujours être considérée comme non autorisée.[27]

Il est en effet possible que l'authentification confirme l'utilisation de l'instrument de paiement et du code correspondant, sans que ce soit pour autant le payeur qui a utilisé cet instrument (et sans que ce soit donc le payeur lui-même qui a donné son consentement).

Plus concrètement, lorsqu'une personne est victime de *phishing* et qu'elle a communiqué au fraudeur des données de sécurité personnelles (par exemple le numéro de carte, la date d'expiration et le code de réponse/OTP), soit directement (par exemple par téléphone), soit indirectement (en les introduisant sur un site web vers lequel elle a été dirigée au moyen d'un hyperlien dans un courriel ou un SMS), il s'agit d'une opération de paiement non autorisée. Le payeur n'a alors pas donné lui-même son consentement à l'exécution de l'ordre de paiement. Il n'a pas donné l'ordre de transférer un montant déterminé sur un compte déterminé (ce qui constitue l'essence d'un ordre de paiement). Il a seulement donné accès à des données (par exemple par téléphone ou en ligne), permettant d'initier une opération de paiement non autorisée ou d'installer une application de paiement.

La question de savoir à qui incombait dans ce cas la charge de la preuve demeurait également incertaine.[28] La Cour de justice s'est aussi prononcée sur ce point: la charge de la preuve incombe au prestataire de services de paiement. Celui-ci doit démontrer que l'utilisateur a donné son consentement dans la forme convenue. La simple utilisation d'un instrument de paiement ne suffit pas à cet égard.[29]

---

27 Hof van Justitie, 11 juli 2024, C-409/22, *Eurobank Bulgaria*, ECLI:EU:C:2024:600, §§ 60-61. "Hoewel het in deze zaak ging om een bijzondere situatie waarin de betalingsopdracht werd gegeven door een fraudeur die een volmacht had vervalst, maakt een grondige lezing van het arrest duidelijk dat het Hof de draagwijdte van het arrest niet tot dergelijke situaties heeft willen beperken." R. Steennot, "Betaalfraude: a never-ending story?", *TBH* 2025, afl. 1, nr. 12.

28 R. Steennot, "Betaalfraude: a never-ending story?", *TBH* 2025, afl. 1, nr. 13. Steennot argumenteert dat het volstaat dat de betaler aannemelijk maakt dat hij/zij geen instemming heeft verleend op basis van elementen zoals het geven van een gedetailleerde beschrijving van de *modus operandi* van de fraudeur, het neerleggen van een klacht bij de politie; Zie ook Bergen 1 oktober 2024. Voor een strengere benadering, zie G. HEIRMAN en L. COENEN, "Phishing: van het (niet-)toegestane karakter van de betalingstransacties tot de beoordeling van de grove nalatigheid," *BFR* 2022, 252.

29 Hof van Justitie, 11 juli 2024, C-409/22, *Eurobank Bulgaria*, ECLI:EU:C:2024:600, §§ 62-63. Deze benadering werd reeds gehanteerd in de rechtspraak van de ondernemingsrechtbank te Antwerpen, zie Orb. Antwerpen (afd. Antwerpen) 6 november 2023, Orb. Antwerpen (afd. Antwerpen) 8 januari 2024, Orb. Antwerpen (afd. Antwerpen) 3 juni 2024.

27 Cour de justice, 11 juillet 2024, C-409/22, *Eurobank Bulgaria*, ECLI:EU:C:2024:600, §§ 60-61. "Bien que, en l'espèce, l'affaire concernait une situation particulière dans laquelle l'ordre de paiement avait été donné par un fraudeur ayant falsifié une procuration, une lecture attentive de l'arrêt révèle que la Cour n'a pas entendu limiter la portée de celui-ci à ce seul type de situations." (*traduction*). R. Steennot, "Betaalfraude: a never-ending story?", RDC 2025, n° 1, 12.

28 R. Steennot, "Betaalfraude: a never-ending story?", *RDC* 2025, n° 1, 13. Steennot fait valoir qu'il suffit que le payeur démontre de manière crédible qu'il n'a pas donné son consentement, en s'appuyant sur des éléments tels qu'une description détaillée du mode opératoire du fraudeur ou le dépôt d'une plainte auprès de la police; voir également Mons, 1er octobre 2024. Pour une approche plus stricte, voir G. HEIRMAN et L. COENEN, "Phishing: van het (niet-)toegestane karakter van de betalingstransacties tot de beoordeling van de grove nalatigheid", DBF 2022, 252.

29 Cour de justice, 11 juillet 2024, C-409/22, *Eurobank Bulgaria*, ECLI:EU:C:2024:600, §§ 62-63. Cette approche a déjà été adoptée dans la jurisprudence du tribunal de l'entreprise d'Anvers, voir tribunal de l'entreprise Anvers (div. Anvers), 6 novembre 2023; tribunal de l'entreprise Anvers (div. Anvers), 8 janvier 2024; tribunal de l'entreprise Anvers (div. Anvers), 3 juin 2024.

Dit wetsvoorstel strekt ertoe de verduidelijking uit voormelde rechtspraak te verankeren in het wettelijk kader. In de rechtspraak werd reeds opgemerkt dat meer houvast geboden zou zijn indien uitdrukkelijk werd bepaald dat van een toegestane betalingstransactie slechts sprake kan zijn wanneer de betaler *zelf* heeft ingestemd met de opdracht.[30] Dit wetsvoorstel geeft gehoor aan die oproep door te bepalen dat een betalingstransactie slechts als toegestaan kan worden aangemerkt indien de betaler zelf uitdrukkelijk heeft ingestemd met de uitvoering van de betalingsopdracht.

6.2. ***Onmiddellijke terugbetaling en grove nalatigheid***

Artikel VII.43 WER bepaalt dat een betalingsdienstaanbieder in het geval van een niet-toegestane transactie verplicht is om de verliezen onmiddellijk terug te betalen. Deze onmiddellijke terugbetaling verhindert niet dat de betalingsdienstaanbieder vervolgens nog een onderzoek uitvoert naar de feiten en de desgevallende aansprakelijkheidsregeling tussen betaler en betalingsdienstaanbieder.

De enige uitzondering op deze onmiddellijke terugbetalingsverplichting bestaat wanneer de betalingsdienstaanbieder redelijke gronden heeft om fraude te vermoeden in hoofde van de betaler en deze gronden ook schriftelijk meedeelt aan de FOD Economie.

Aldus geldt de onmiddellijke terugbetalingsverplichting onverkort wanneer er een vermoeden of mogelijkheid bestaat dat de betaler een of meer van zijn/haar verplichtingen niet is nagekomen, ook door grove nalatigheid. Dit stemt overeen met de Europese regelgeving, zoals geïnterpreteerd door de advocaat-generaal bij het Hof van Justitie.[31] De ondernemingsrechtbank te Brussel stelt zeer duidelijk dat een andere interpretatie het beschermingsmechanisme ten aanzien van de betaler zou uithollen, “omdat artikel VII.43 WER bijna nooit zou kunnen worden toegepast en daarmee afbreuk zou worden gedaan aan de bedoeling van de wetgever en aan de beschermingsgedachte die aan de PSD2-richtlijn ten grondslag ligt.”[32]

Dit wetsvoorstel verduidelijkt art. VII.43, § 1, eerste lid, WER door uitdrukkelijk te bepalen dat een vermoeden van grove nalatigheid geen grond vormt om de onmiddellijke

La présente proposition de loi vise à ancrer les précisions apportées par la jurisprudence précitée dans le cadre légal. Il a déjà été observé dans la jurisprudence qu’il serait préférable de préciser explicitement qu’une opération de paiement ne peut être considérée comme ayant été autorisée que si le payeur a *lui-même* consenti à l’ordre de paiement.[30] La présente proposition de loi répond à cette observation en prévoyant qu’une opération de paiement ne peut être considérée comme ayant été autorisée que lorsque le payeur a lui-même explicitement consenti à l’exécution de l’ordre de paiement.

6.2. ***Remboursement immédiat et négligence grave***

L’article VII.43 du CDE dispose qu’en cas d’opération de paiement non autorisée, le prestataire de services de paiement doit rembourser immédiatement au payeur le montant des pertes subies. Ce remboursement immédiat n’empêche pas le prestataire de services de paiement de mener par la suite une enquête sur les faits et de déterminer, le cas échéant, le régime de responsabilité entre le payeur et le prestataire de services de paiement.

Il peut être dérogé à cette obligation de remboursement immédiat dans un seul cas, à savoir lorsque le prestataire de services de paiement a de bonnes raisons de soupçonner une fraude de la part du payeur et qu’il communique ces raisons par écrit au SPF Économie.

L’obligation de remboursement immédiat s’applique donc sans restriction lorsqu’il existe une présomption ou une possibilité que le payeur n’ait pas satisfait à une ou plusieurs des obligations qui lui incombent, y compris à la suite d’une négligence grave. Cela est conforme à la réglementation européenne, telle qu’interprétée par l’avocat général à la Cour de justice.[31] Le tribunal de l’entreprise de Bruxelles indique très clairement qu’une autre interprétation viderait de sa substance le mécanisme de protection du payeur, “car l’article VII.43 du Code de droit économique ne pourrait presque jamais être appliqué et qu’il y aurait ainsi atteinte à l’intention du législateur et au principe de protection qui sous-tend la directive DSP2” (*traduction*)[32].

La présente proposition de loi précise la portée de l’article VII.43, § 1er, premier alinéa, du CDE en prévoyant expressément qu’une présomption de négligence grave

30 R. Steennot, “Betaalfraude: a never-ending story?”, *TBH* 2025, afl. 1, nr. 19.

31 Conclusie van advocaat-generaal A. RANTOS van 25 september 2025, zaak C-337/22, N.O. tegen PKO Bank Polski S.A., ECLI:EU:C:2025:720, §§ 26-29.

32 Ondernemingsrechtbank Brussel, 16 oktober 2025, A/24/02.457, nr. 14.

30 R. Steennot, “Betaalfraude: a never-ending story?”, RDC 2025, n° 1, 19.

31 Conclusion de l’avocat général A. RANTOS du 25 septembre 2025, affaire C-337/22, N.O. contre PKO Bank Polski S.A., ECLI:EU:C:2025:720, §§ 26-29.

32 Tribunal de l’entreprise de Bruxelles, 16 octobre 2025, A/24/02.457, n° 14.

terugbetalingsverplichting te weigeren of op te schorten bij niet-toegestane transacties.

6.3. ***Verwijlinteresten***

Met het voorgestelde 3° in artikel 3 voert dit wetsvoorstel verwijlintresten in, dit ingeval van latere herkwalificatie van de transactie door de rechtbank én bij het niet-respecteren van restitutieplicht, wat voor dit laatste impliceert dat we het voorbeeld volgen van Frankrijk dat dit reeds heeft voorzien bij de omzetting van de Europese richtlijn in 2018.

Omdat de bescherming voor de consument bij een toegestane transactie momenteel vrijwel onbestaande is, proberen banken niet-toegestane transacties (zoals bij phishing) vaak systematisch als "toegestaan" te bestempelen om zo hun aansprakelijkheid te ontlopen. Hierdoor wordt de consument de wettelijke bescherming ontnomen en wordt hij gedwongen om een lange en dure juridische procedure te starten om zijn gelijk te halen. Een uitspraak in eerste aanleg duurt gemiddeld 528 dagen, en een uitspraak in beroep gebeurt gemiddeld 4,5 jaar na de feiten. Wanneer de rechter de transactie maanden of jaren later alsnog herkwalificeert naar een "niet-toegestane transactie" (zoals recent gebeurde bij het hof van beroep in Antwerpen[33]), heeft het slachtoffer al die tijd onterecht niet over zijn of haar financiële middelen kunnen beschikken.

Door wettelijk vast te leggen dat er van rechtswege en zonder ingebrekestelling verwijlintresten verschuldigd zijn, wordt de consument financieel gecompenseerd voor de periode dat hij zijn geld heeft moeten missen door de onterechte weigering van de bank. Dit ontmoedigt banken ook om transacties lichtzinnig of strategisch als "toegestaan" te kwalificeren puur om de terugbetaling te vertragen.

Artikel VII.43 WER (gebaseerd op artikel 73 PSD2) verplicht banken om het bedrag van een niet-toegestane transactie onmiddellijk (uiterlijk op de volgende werkdag) terug te betalen. De enige uitzondering hierop is wanneer de bank een gegrond vermoeden van fraude door de betaler zelf heeft en dit meldt aan de FOD Economie. In de praktijk is deze regel echter een dode letter geworden. Banken weigeren de onmiddellijke terugbetaling systematisch door zich te beroepen op een vermeende "grove nalatigheid" van het slachtoffer.

[33] Antwerpen 3 september 2025, NjW 2025, afl. 531, 808.

ne constitue pas un motif permettant de refuser ou de suspendre l'obligation de remboursement immédiat en cas d'opérations de paiement non autorisées.

6.3. ***Intérêts de retard***

L'article 3, 3°, de la présente proposition de loi prévoit d'appliquer des intérêts de retard en cas de requalification ultérieure de la transaction par le tribunal et de non-respect de l'obligation de restitution. Pour ce dernier point, elle suit donc l'exemple de la France, qui a prévu un mécanisme similaire dès la transposition de la directive européenne en 2018.

Étant donné que la protection du consommateur est actuellement quasi inexistante en cas d'opération de paiement autorisée, les banques tentent souvent de qualifier systématiquement d'"autorisées" les opérations de paiement non autorisées (comme dans le cas du *phishing*) afin d'échapper à leur responsabilité. Le consommateur se voit ainsi privé de la protection légale et contraint d'engager une longue et coûteuse procédure judiciaire pour faire valoir ses droits. Un jugement en première instance prend en moyenne 528 jours, et un jugement en appel intervient en moyenne 4,5 ans après les faits. Lorsque le juge requalifie l'opération, des mois ou des années plus tard, en "opération non autorisée" (comme ce fut le cas récemment devant la Cour d'appel d'Anvers[33]), ce jugement intervient à l'issue d'une longue période durant laquelle la victime a été indûment privée de la possibilité de disposer de ses ressources financières.

En ancrant dans la loi la règle selon laquelle des intérêts de retard sont dus de plein droit et sans mise en demeure, la présente proposition vise à dédommager financièrement le consommateur pour la période durant laquelle il a été privé de son argent en raison du refus injustifié de la banque. Le but est également de dissuader les banques de qualifier à la légère ou par pure stratégie des opérations de paiement d'"autorisées" dans le seul but de retarder le remboursement.

L'article VII.43 du CDE (basé sur l'article 73 de la directive DSP2) oblige les banques à rembourser immédiatement (au plus tard le jour ouvrable suivant) le montant d'une opération de paiement non autorisée, sauf – seule et unique exception – si la banque a de bonnes raisons de soupçonner une fraude de la part du payeur lui-même et qu'elle le signale au SPF Économie. Dans la pratique, toutefois, cette règle est restée lettre morte. Les banques refusent systématiquement le remboursement immédiat en invoquant une prétendue "négligence grave" de la part de la victime.

[33] Anvers 3 septembre 2025, NjW 2025, n° 531, 808.

Zelfs de Ombudsman voor financiële diensten (Ombudsfin) hekelt deze gang van zaken. De Ombudsman wijst erop dat de banken de 24-uurregel systematisch negeren door eenvoudig en zonder onmiddellijk bewijs "grove nalatigheid" in te roepen. Hierdoor wordt de wettelijke bewijslast omgekeerd: niet de bank moet bewijzen dat de klant in de fout ging alvorens de terugbetaling te weigeren, maar de klant moet maanden- of jarenlang procederen om zijn eigen geld terug te zien[34]. Zelfs wanneer Ombudsfin een dossier gegrond verklaart, weigert een meerderheid van de banken nog steeds de onmiddellijke restitutie[35].

Zoals de advocaat-generaal onlangs verduidelijkte in een zaak voor het Europees Hof van Justitie, mag een bank de onmiddellijke terugbetaling echter niet opschorten op basis van grove nalatigheid[36].

Dit wetsvoorstel verankert het fundamentele principe "eerst betalen, dan pas argumenteren", zoals bepleit door de advocaat-generaal van het Hof van Justitie, om de positie van de consument bij betaalfraude effectief te beschermen. Op grond van artikel VII.43 WER is een betalingsdienstaanbieder immers verplicht om een niet-toegestane transactie onmiddellijk terug te betalen. De bank kan deze termijn uitsluitend opschorten wanneer er een schriftelijk en onderbouwd vermoeden van fraude door de betaler zelf bestaat, dat formeel is gemeld aan de FOD Economie.

Om de naleving van deze restitutieplicht af te dwingen, wordt artikel VII.43, § 1, WER aangevuld met een sanctieregime van automatische verwijlintresten. Indien de bank de onmiddellijke restitutieplicht niet respecteert, is zij voortaan van rechtswege en zonder voorafgaande ingebrekestelling verwijlintresten verschuldigd. Deze interesten zijn eveneens verschuldigd in situaties waarin een transactie pas in een later stadium door een rechtbank wordt geherkwalificeerd als niet-toegestaan (*supra*).

6.4. ***Strengere handhaving***

De naleving van de terugbetalingsverplichting moet gepaard gaan met handhaving. Het is essentieel dat de toezichthouder, met name de FOD Economie, daadkrachtig kan optreden om ervoor te zorgen dat deze terugbetalingsverplichting daadwerkelijk wordt toegepast.

[34] Ombudsman trekt aan de alarmbel: banken negeren massaal de wetgeving rond phishing", *vrt.be*, 18 november 2025, *https://www.vrt.be/vrtnws/nl/2025/11/18/phishing-banken-wetgeving/*

[35] Ombudsfin, Jaarverslag 2022, Brussel, 2022, blz. 21-23.

[36] Conclusie van advocaat-generaal A. RANTOS van 25 september 2025, zaak C-337/22, N.O. tegen PKO Bank Polski S.A., ECLI:EU:C:2025:720

Même le Médiateur des services financiers (Ombudsfin) déplore vivement cette situation. Il attire l'attention sur le fait que les banques ignorent systématiquement la règle des 24 heures en invoquant simplement, et sans preuve immédiate, une "négligence grave", renversant ainsi la charge de la preuve légale: la banque ne doit pas prouver, avant de refuser le remboursement, que le client a commis une faute, mais le client doit procéder en justice pendant des mois, voire des années, pour récupérer son argent[34]. Même lorsqu'Ombudsfin déclare un dossier fondé, une majorité de banques refuse encore le remboursement immédiat[35].

Comme l'a récemment précisé l'avocat général dans une affaire devant la Cour de justice de l'Union européenne, une banque ne peut toutefois pas suspendre le remboursement immédiat au motif d'une négligence grave[36].

La présente proposition de loi consacre le principe fondamental "payer d'abord, contester ensuite", tel que plaidé par l'avocat général de la Cour de justice, afin de protéger de manière effective la position du consommateur en cas de fraude aux paiements. En vertu de l'article VII.43 du CDE, un prestataire de services de paiement doit en effet rembourser immédiatement le montant d'une opération de paiement non autorisée. La banque ne peut suspendre ce délai que s'il existe un soupçon écrit et fondé de fraude de la part du payeur lui-même, qui a été formellement signalé au SPF Économie.

Afin de garantir le respect de cette obligation de remboursement, l'article VII.43, § 1er, du CDE est complété par un régime de sanction prévoyant des intérêts de retard automatiques. Si la banque ne respecte pas l'obligation de remboursement immédiat, elle est désormais redevable d'intérêts de retard de plein droit et sans mise en demeure préalable. Ces intérêts sont également dus dans les cas où une opération de paiement n'est requalifiée de non autorisée par un tribunal qu'à un stade ultérieur (*supra*).

6.4. ***Répression plus stricte***

Le respect de l'obligation de remboursement doit aller de pair avec la répression. Il est essentiel que l'autorité de surveillance, à savoir le SPF Économie, puisse intervenir avec fermeté pour faire en sorte que cette obligation de paiement soit effectivement appliquée.

[34] Ombudsman trekt aan de alarmbel: banken negeren massaal de wetgeving rond phishing", *vrt.be*, 18 novembre 2025, *https://www.vrt.be/vrtnws/nl/2025/11/18/phishing-banken-wetgeving/*

[35] Ombudsfin, Rapport annuel 2022, Bruxelles, 2022, p. 21-23.

[36] Conclusion de l'avocat général A. RANTOS du 25 septembre 2025, affaire C-337/22, N.O. contre PKO Bank Polski S.A., ECLI:EU:C:2025:720

Om te voorkomen dat deze wettelijke verplichting genegeerd wordt, voert dit wetsvoorstel een wijziging door aan artikel XV.89 WER. We stellen de toezichthouder in staat om effectieve administratieve geldboetes en strafrechtelijke sancties op te leggen aan financiële instellingen die de wettelijke terugbetalingsverplichting negeren. Hiermee wordt voorkomen dat de restitutieplicht, die essentieel is voor de consumentenbescherming, dode letter blijft.

6.5. ***Transparantie en strikte termijnen***

Wanneer slachtoffers van phishing de fraude melden bij hun bank, belanden zij vandaag te vaak in een tergend lange onzekerheid. Wanneer we de huidige bepalingen van het Wetboek van economisch recht analyseren, zien we dat de wetgever op diverse plaatsen al zeer strikte termijnen heeft ingebouwd om de consument te beschermen en rechtszekerheid te bieden:

— 13 maanden voor de consument: een betalingsdienstgebruiker heeft tot maximaal 13 maanden de tijd om een niet-toegestane transactie te betwisten en rechtzetting te eisen (artikel VII. 41, § 1, WER);

— 1 werkdag voor de bank ("*pay first, argue later*"): bij een niet-toegestane transactie moet de bank in theorie onmiddellijk en uiterlijk aan het einde van de eerstvolgende werkdag, het bedrag terugbetalen (artikel VII. 43, § 1, WER);

— 10 werkdagen voor betwiste domiciliëringen: bij specifieke toegestane transacties die door de begunstigde worden geïnitieerd, heeft de consument 8 weken de tijd om een terugbetaling te vragen. De bank moet vervolgens binnen de 10 werkdagen het volledige bedrag terugbetalen of haar weigering motiveren met opgave van de instanties (zoals de ombudsdienst en de FOD Economie) waar de betaler de zaak aanhangig kan maken (artikel VII. 47, §§ 1 en 2 WER);

— 15 werkdagen voor algemene klachten: voor algemene klachten over betalingsdiensten moet de bank binnen 15 werkdagen reageren. Enkel in uitzonderlijke situaties mag dit verlengd worden tot maximaal 35 werkdagen (artikel VII. 55/14 WER).

Ondanks deze waaier aan wettelijke termijnen, valt het slachtoffer van phishing vandaag in een procedureel zwart gat. Banken weigeren de onmiddellijke terugbetaling van één werkdag systematisch, hetzij door eenvoudig te oordelen dat de transactie door de klant "toegestaan"

Pour éviter que cette obligation légale soit ignorée, la présente proposition de loi apporte une modification à l'article XV.89 CDE. Elle habilite l'autorité de surveillance à infliger des amendes administratives effectives et des sanctions pénales aux établissements financiers qui ignorent l'obligation de remboursement. Le but est d'éviter ainsi que l'obligation de restitution, qui est essentielle pour la protection du consommateur, reste lettre morte.

6.5. ***Transparence et délais stricts***

Aujourd'hui, lorsque les victimes de *phishing* signalent la fraude à leur banque, elles se retrouvent trop souvent dans une situation d'incertitude qui s'éternise. Une analyse des dispositions actuelles du Code de droit économique montre que le législateur a déjà prévu, dans plusieurs dispositions, des délais très stricts afin de protéger le consommateur et de lui offrir une sécurité juridique:

— 13 mois pour le consommateur: un utilisateur de services de paiement dispose d'un délai de 13 mois au maximum pour contester une opération non autorisée et exiger la correction (article VII. 41, § 1er, CDE);

— 1 jour ouvrable pour la banque ("payer d'abord, contester ensuite"): en cas d'opération de paiement non autorisée, la banque doit, en théorie, rembourser le montant immédiatement et au plus tard à la fin du premier jour ouvrable suivant (article VII. 43, § 1er, CDE);

— 10 jours ouvrables pour des domiciliations contestées: en cas d'opérations de paiement autorisées spécifiques, qui ont été initiées par le bénéficiaire, le consommateur dispose d'un délai de huit semaines pour demander le remboursement. Dans un délai de dix jours ouvrables suivant la réception de la demande de remboursement, la banque soit rembourse le montant total de l'opération de paiement, soit justifie son refus de rembourser, en indiquant les organismes (comme le Service de médiation ou le SPF Économie) que le payeur peut alors saisir (article VII. 47, §§ 1er et 2, CDE);

— 15 jours ouvrables pour les plaintes générales: pour les plaintes générales concernant les services de paiement, la banque doit réagir dans les 15 jours ouvrables. Ce délai peut être porté à 35 jours ouvrables maximum dans des situations exceptionnelles (article VII. 55/14, CDE).

En dépit de cet éventail de délais légaux, la victime d'une tentative de *phishing* est confrontée à l'heure actuelle à un vide juridique du point de vue procédural. Les banques refusent systématiquement le remboursement immédiat dans le délai d'un jour ouvrable, soit en

was, hetzij door zonder onmiddellijk bewijs een “grove nalatigheid” in te roepen.

Omdat de bank de 1-dag termijn negeert, valt het fraudedossier terug in de “algemene klachtenprocedure” van 15 tot 35 werkdagen. Hierdoor wordt het slachtoffer weken- of zelfs maandenlang in het ongewisse gelaten over de stand van het fraudeonderzoek. Wanneer het antwoord eindelijk volgt, betreft dit vaak een summiere, standaard weigeringsbrief, zonder duidelijk vermelding van de exacte juridische gronden voor de weigering (toegestaan vs. niet-toegestaan) of de rechten die de consument nog kan uitputten.

Consumenten zijn immers zelden op de hoogte van hun recht om kosteloos beroep te doen op Ombudsfin. Dat de weg naar deze ombudsdienst onvoldoende gekend is, blijkt uit de cijfers. Terwijl de veiligheidsmonitor aantoont dat bijna de helft van de bevolking doelwit is van phishing en we weten dat er jaarlijks honderden miljoenen euro’s gestolen worden, behandelde Ombudsfin in 2024 in heel België welgeteld slecht 789 ontvankelijke klachten inzake betwiste verrichtingen na phishing of andere online fraude[37]. Dit uiterst lage aantal dossiers is absoluut *nihil* in vergelijking met de vele slachtoffers. Hieruit kan afgeleid worden dat Ombudsfin simpelweg niet goed bekend is bij de burger, mede doordat banken bij weigering tot terugbetaling nalaten om het slachtoffer proactief naar deze instantie door te verwijzen.

Dit voorstel maakt een einde aan deze onzekerheid door een strikte termijn in te voeren en er een informatieplicht aan te koppelen.

Het voorstel verplicht de bank om in elk geval (kwalificatie toegestaan of niet-toegestaan) binnen een termijn van 10 werkdagen een uitgebreide en gemotiveerde beslissing af te leveren aan de consument. Hiermee wordt de regeling voor phishing gelijkgeschakeld met de reeds bestaande termijn van 10 werkdagen voor betwiste domiciliëringen. Bovendien anticipeert dit op de bepalingen uit het nieuwe Europese voorstel voor een *Payment Services Regulation*, dat eveneens een onderzoeks- en motiveringtermijn van 10 werkdagen naar voren schuift bij onderzoek naar vermoeden van fraude[38].

Daarnaast wordt de bank verplicht om proactief en transparant te communiceren. De consument moet op

[37] Ombudsfin, Jaarverslag 2024, Brussel, 2025, p. 16.
[38] R. Steennot, “Betaalfraude: a never ending story?”, TBH 2025, afl. 1, nr. 25.

considérant simplement que l’opération était “autorisée” par le client, soit en invoquant une “négligence grave” sans preuve immédiate.

La banque faisant fi du délai d’un jour, le dossier de fraude retombe dans la “procédure générale de réclamation” de 15 à 35 jours ouvrables. La victime est donc dans l’incertitude pendant des semaines, voire des mois, au sujet de l’état d’avancement de l’enquête sur la fraude. Lorsque la réponse arrive enfin, il s’agit souvent d’une lettre de refus succincte et standardisée, qui ne mentionne pas clairement les fondements juridiques exacts du refus (opération autorisée/opération non autorisée) ni les voies de recours dont le consommateur dispose encore.

En effet, les consommateurs ignorent souvent qu’ils ont le droit de faire appel sans frais à Ombudsfin. Les chiffres montrent que ce service de médiation est trop peu connu. Alors que près de la moitié de la population est victime de *phishing* selon le Moniteur de sécurité et que des centaines de millions d’euros sont volés chaque année, Ombudsfin n’a traité en 2024, pour toute la Belgique, que 789 plaintes recevables concernant des opérations contestées à la suite d’un *phishing* ou d’autres fraudes en ligne[37]. Ce nombre extrêmement faible de dossiers est absolument insignifiant par rapport au nombre élevé de victimes. On peut en déduire qu’Ombudsfin n’est tout simplement pas bien connu du grand public, notamment parce que les banques, lorsqu’elles refusent un remboursement, omettent d’orienter proactivement la victime vers cette instance.

La présente proposition met fin à cette incertitude en instaurant un délai strict et en assortissant celui-ci d’une obligation d’information.

La proposition impose à la banque l’obligation de communiquer au consommateur en tous les cas (qu’il s’agisse d’une qualification “autorisée” ou “non autorisée”) une décision détaillée et motivée dans un délai de 10 jours ouvrables. La réglementation sur le *phishing* sera ainsi alignée sur celle relative aux domiciliations contestées dans laquelle le délai existant est déjà de 10 jours ouvrables. De plus, cela permettra d’anticiper sur les dispositions du nouveau projet européen de règlement sur les services de paiement qui préconise aussi un délai d’examen et de motivation de 10 jours ouvrables en cas d’enquête sur une suspicion de fraude[38].

Une autre obligation imposée à la banque est celle de communiquer de manière proactive et transparente. Elle

[37] Ombudsfin, Rapport annuel 2024, Bruxellles, 2025, p. 16.
[38] R. Steennot, “Betaalfraude: a never-ending story?”, RDC 2025, n° 1, 25.

een duurzame drager in klare taal worden geïnformeerd over zijn dossier. Dit individueel dossier bevat minstens:

— de juridische kwalificatie van de transactie als toegestaan dan wel niet-toegestaan, met een expliciete motivering gebaseerd op de feitelijke instemming van de betaler met het bedrag en de unieke identificator;

— de technische bewijsstukken van de authenticatie en de registratie van de transactie;

— de bank dient transparant aan te tonen welke concrete veiligheidsmaatregelen zij heeft genomen om het geld van haar klant te beschermen. Zoals recente rechtspraak aantoont, kan een gebrekkige fraudedetectie immers leiden tot aansprakelijkheid van de bank[39]. Slachtoffers hebben het recht om te weten of de bank haar algemene zorgplicht is nagekomen[40]. De bank moet dus in haar beslissing verantwoorden of en hoe zij het afwijkende uitgavenpatroon, de locatie of het apparaatgebruik van de betaler heeft gemonitord;

— verwijzing naar de bevoegde geschilleninstanties, met name Ombudsfin en de FOD Economie.

Tot slot dient benadrukt te worden dat ingevolge artikel 1.2 van het nieuwe Burgerlijk Wetboek het artikel 2 en de voorgestelde punten 1° en 2° van artikel 3 onmiddellijk van toepassing zijn, ook op lopende zaken waarvoor er nog geen rechterlijke beslissing is die kracht van gewijsde heeft gekregen.

Jeroen Soete (Vooruit)

doit fournir au consommateur les informations relatives à son dossier, sur un support durable et dans un langage clair. Ce dossier individuel contient au moins:

— la qualification juridique de l'opération (autorisée ou non), accompagnée d'une motivation explicite fondée sur le consentement effectif du payeur quant au montant et à l'identifiant unique;

— les pièces justificatives techniques de l'authentification et de l'enregistrement de l'opération;

— la banque doit démontrer de manière transparente quelles mesures de sécurité concrètes elle a prises pour protéger l'argent de son client. Comme la jurisprudence récente en atteste, une détection défaillante de la fraude peut en effet engager la responsabilité de la banque[39]. Les victimes ont le droit de savoir si la banque a respecté son devoir général de vigilance[40]. Dans sa décision, la banque doit donc indiquer si elle a surveillé le comportement inhabituel du payeur en matière de dépenses, la localisation ou l'utilisation de son appareil, et comment elle a procédé à cet effet;

— la mention des instances de recours compétentes, notamment Ombudsfin et le SPF Économie.

Enfin, il convient de souligner qu'en vertu de l'article 1.2 du nouveau Code civil, l'article 2 et les points 1° et 2° proposés à l'article 3 s'appliqueront immédiatement, y compris aux affaires pendantes pour lesquelles aucune décision judiciaire coulée en force de chose jugée n'a encore été rendue.

39 Een treffend voorbeeld hiervan is het recente 'Itsme-vonnis' van de Nederlandstalige ondernemingsrechtbank van Brussel (4 januari 2024), waarbij de bank aansprakelijk werd gesteld omdat de fraudeur op zeer korte tijd maar liefst 97 frauduleuze transacties kon uitvoeren zonder dat het fraudesysteem van de bank ingreep. 243 Rb. Brussel (NL), 4 januari 2024, DBF-BFR 2024/2.

40 Ook Hof van Beroep te Antwerpen oordeelde onlangs dat het niet (of onvoldoende) waarschuwen van een klant wanneer fraudeurs een mobiele bank-app op een nieuw toestel installeren, wijst op een ernstig en zwaarwichtig falen van het IT-systeem en het fraudedetectiesysteem van de bank. HvB Antwerpen 3 september 2025, NjW, 2025, afl. 531, 808.

39 Un exemple frappant en est le récent "jugement Itsme" rendu par le tribunal néerlandophone de l'entreprise de Bruxelles (4 janvier 2024), dans lequel la banque a été déclarée responsable parce que le fraudeur a pu effectuer pas moins de 97 opérations frauduleuses en très peu de temps sans que le système antifraude de la banque n'intervienne. 243 Tribunal de Bruxelles (NL), 4 janvier 2024, DBF-BFR 2024/2.

40 Récemment, la Cour d'appel d'Anvers a estimé elle aussi que le fait de ne pas avertir (ou de ne pas avertir suffisamment) un client lorsque des fraudeurs installent une application bancaire mobile sur un nouvel appareil témoigne d'une défaillance grave et importante du système informatique et du système de détection des fraudes de la banque. Cour d'appel d'Anvers, 3 septembre 2025, *NjW*, 2025, n° 531, 808.

WETSVOORSTEL

Artikel 1

Deze wet regelt een aangelegenheid als bedoeld in artikel 74 van de Grondwet.

Art. 2

In artikel VII.32, § 1, eerste lid, van het Wetboek van economisch recht, vervangen bij de wet van 19 juli 2018, wordt het woord “zelf” ingevoegd tussen het woord “betaler” en de woorden “heeft ingestemd”.

Art. 3

In artikel VII.43 van hetzelfde Wetboek, vervangen bij de wet van 19 juli 2018, worden de volgende wijzigingen aangebracht:

1° paragraaf 1, eerste lid, wordt aangevuld met de volgende zin:

“Een vermoeden van grove nalatigheid in hoofde van de betaler vormt geen grond tot weigering of uitstel van de onmiddellijke betaling door de betalingsdienstaanbieder.”;

2° in paragraaf 1 worden tussen het tweede en het derde lid twee leden ingevoegd, luidende:

“Indien de betalingsdienstaanbieder de onmiddellijke terugbetaling weigert of opschort – ongeacht of hij de transactie kwalificeert als een toegestane dan wel een niet-toegestane transactie – stelt hij de betalingsdienstgebruiker hiervan in kennis uiterlijk op de tiende werkdag na de ontvangst van de in artikel VII.41 bedoelde kennisgeving, kosteloos en op papier of op een andere duurzame gegevensdrager.

De aan de betalingsdienstgebruiker te verstrekken informatie in deze kennisgeving bevat minstens de volgende elementen betreffende:

1° de specifieke gronden en de rechtvaardiging van de beslissing tot weigering of opschorting, waarbij in gemakkelijk te begrijpen bewoordingen en in duidelijke en bevattelijke vorm wordt omschreven of de weigering of opschorting steunt op het toegestane of niet-toegestane karakter, dan wel op fraude in hoofde van de betaler;

PROPOSITION DE LOI

Article 1er

La présente loi règle une matière visée à l’article 74 de la Constitution.

Art. 2

À l’article VII.32, § 1er, alinéa 1er, du Code de droit économique, remplacé par la loi du 19 juillet 2018, le mot “lui-même” est inséré entre le mot “a” et les mots “donné son consentement”.

Art. 3

À l’article VII.43 du même Code, remplacé par la loi du 19 juillet 2018, les modifications suivantes sont apportées:

1° le paragraphe 1er, alinéa 1er, est complété par la phrase suivante:

“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.”;

2° au paragraphe 1er, deux alinéas rédigés comme suit sont insérés entre les alinéas 2 et 3:

“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° de technische bewijsstukken van de authenticatie en de registratie van de betwiste transactie;

3° een verantwoording waaruit blijkt op welke wijze de betalingsdienstaanbieder aan zijn algemene zorgvuldigheidsplicht is tegemoetgekomen en hoe zijn fraudedetectiesysteem met betrekking tot deze transactie heeft gewerkt;

4° de aansprakelijkheid van de betaler overeenkomstig artikel VII.44, met inbegrip van de gegevens over het betrokken bedrag;

5° de klachten- en buitengerechtelijke geschillenregelingen die voor de betalingsdienstgebruiker overeenkomstig boek XVI openstaan, met inbegrip van het geografische adres van de instelling waartoe de betalingsdienstgebruiker zijn klachten kan richten, waaronder het bevoegde orgaan bedoeld in artikel VII.216 en de contactgegevens van de Algemene Directie Economische Inspectie bij de FOD Economie.";

3° paragraaf 1 wordt aangevuld met twee leden, luidende:

"Indien de terugbetaling niet gebeurt binnen de termijn bepaald in het eerste lid, is de betalingsdienstaanbieder van rechtswege en zonder ingebrekestelling verwijlinteresten verschuldigd. Deze interesten bedragen:

— de wettelijke intrestvoet, verhoogd met 5 procentpunten vanaf de eerste dag vertraging;

— verhoogd met 10 procentpunten vanaf de achtste dag vertraging;

— verhoogd met 15 procentpunten vanaf de dertigste dag vertraging.

De interesten worden automatisch berekend en toegevoegd aan het terug te betalen bedrag."

Art. 4

In artikel XV.89 van hetzelfde Wetboek, laatstelijk gewijzigd bij de wet van 11 december 2025, wordt de bepaling onder 17° vervangen als volgt:

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.";

3° le paragraphe 1er est complété par deux alinéas rédigés comme suit:

"Si le remboursement n'est pas effectué dans le délai fixé à l'alinéa 1er, le prestataire de services de paiement est redevable, de plein droit et sans mise en demeure, d'intérêts de retard. Ces intérêts sont calculés:

— au taux d'intérêt légal, majoré de 5 points de pourcentage à compter du premier jour de retard;

— majoré de 10 points de pourcentage à compter du huitième jour de retard;

— majoré de 15 points de pourcentage à compter du trentième jour de retard.

Les intérêts sont calculés automatiquement et ajoutés au montant à rembourser."

Art. 4

À l'article XV.89 du même Code, modifié en dernier lieu par la loi du 11 décembre 2025, le 17° est remplacé par ce qui suit:

"17° van de artikelen VII.43, VII.44 en VII.45, betreffende de voorlopige terugbetalingsverplichting en de volledige en gedeelde aansprakelijkheid van de betalingsdienstaanbieder bij niet-toegestane betalingstransacties."

3 april 2026

Jeroen Soete (Vooruit)

"17° des articles VII.43, VII.44 et VII.45 relatifs à l'obligation de remboursement provisoire et à la responsabilité totale et partagée du prestataire de services de paiement en cas d'opérations de paiement non autorisées."

3 avril 2026

Centrale drukkerij - Imprimerie centrale