DOC 56 **0542/001**

BELGISCHE KAMER VAN VOLKSVERTEGENWOORDIGERS

27 november 2024

WETSVOORSTEL

tot wijziging van enkele artikelen van het Boek VII van het Wetboek van Economisch Recht met het oog op een betere bescherming van de betaler bij bepaalde vormen van fraude

(ingediend door de heer Vincent Van Quickenborne)

CHAMBRE DES REPRÉSENTANTS DE BELGIQUE

27 novembre 2024

PROPOSITION DE LOI

modifiant plusieurs articles du Livre VII du Code de droit économique en vuede mieux protéger le payeur contre certaines formes de fraude

(déposée par M. Vincent Van Quickenborne)

SAMENVATTING

Dit wetsvoorstel beoogt de consument beter te beschermen tegen betaalfraude.

RÉSUMÉ

Cette proposition de loi vise à mieux protéger le consommateur contre la fraude au paiement.

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*
Open Vld	:	*Open Vlaamse liberalen en democraten*
DéFI	:	*Démocrate Fédéraliste Indépendant*

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

TOELICHTING

DAMES EN HEREN,

De laatste jaren zijn verschillende consumenten het slachtoffer geworden van betaalfraude. Sommige onder hen zijn daarbij zeer aanzienlijke bedragen verloren. Deze wet strekt ertoe enerzijds het concept van niet-toegestane betalingstransacties te verduidelijken en anderzijds de aansprakelijkheid van de betaler te beperken voor niet-toegestane elektronische betalingstransacties op afstand ook in geval van grove nalatigheid.

TOELICHTING BIJ DE ARTIKELEN

Artikel 2

Deze wetswijziging strekt ertoe te verduidelijken dat een betalingstransactie maar als toegestaan kan worden aangemerkt indien de betaler zelf heeft ingestemd met de uitvoering van de betalingsopdracht. De loutere vaststelling dat de betaler aan een derde gegevens heeft verstrekt die een derde toelaten een betalingsopdracht te geven, volstaat niet om van een toegestane betalingstransactie te spreken. Dat zou slechts het geval zijn indien die derde gemandateerd was om de betalingsopdracht te geven.

Ook het feit dat een transactie geauthenticeerd werd, i.e. dat zij in de overeengekomen vorm en volgens de overeengekomen procedure werd verleend, verhindert niet dat er sprake is van een niet-toegestane betalingstransactie. 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)[1].

Meer concreet, wanneer iemand het slachtoffer is geworden van phishing en persoonlijke beveiligingsgegevens (bijvoorbeeld het kaartnummer, de vervaldatum en response code/OTP) rechtstreeks (bijvoorbeeld via de telefoon) of onrechtstreeks (door deze in te voeren op een website waarnaar hij via een hyperlink in een e-mail of sms werd geleid) heeft gecommuniceerd aan de fraudeur gaat het om een niet-toegestane betalingstransactie. De betaler heeft alsdan niet zelf zijn instemming

[1] Zie ook HR (Nederland) 21 mei 2021, *TBH* 2022, 169, noot R. Steennot; Luik 9 januari 2020, *DAOR* 2022, afl. 143, 55; Vred. Seraing 14 juni 2021 (onuitg.); B. De Waele, "Betwiste online betalingstransacties: analyse van Ombudsfin", *BFR* 2020/bonus, 37. *Anders*: Rb. Brussel 8 januari 2021, *DAOR* 2022, afl. 141, 102, noot D. Blommaert en E. Corthals).

DÉVELOPPEMENTS

MESDAMES, MESSIEURS,

Ces dernières années, certains consommateurs ont été victimes de fraudes aux paiements qui leur ont parfois fait perdre des sommes considérables. La présente proposition de loi vise, d'une part, à préciser la notion d'opération de paiement non autorisée et, d'autre part, à limiter la responsabilité du payeur dans les opérations de paiement électronique à distance non autorisées, y compris en cas de négligence grave.

COMMENTAIRE DES ARTICLES

Article 2

Cette disposition vise à préciser qu'une opération de paiement ne peut être réputée autorisée que si le payeur a donné lui-même son consentement à l'exécution de l'ordre de paiement. La simple constatation que le payeur a fourni à un tiers des informations permettant à celui-ci de donner un ordre de paiement ne suffit pas pour considérer qu'il est question d'une opération de paiement autorisée. Cela ne serait le cas que si ce tiers avait été mandaté pour donner l'ordre de paiement.

Le fait qu'une opération de paiement ait été authentifiée, c'est-à-dire qu'elle ait été réalisée sous la forme et selon la procédure convenues, n'empêche pas non plus de la considérer comme non autorisée. En effet, il est possible que l'authentification confirme l'utilisation de l'instrument de paiement avec le code correspondant, mais que ce ne soit pas le payeur qui ait utilisé cet instrument (et donc qu'il n'ait pas donné lui-même son consentement).[1]

Plus concrètement, lorsqu'une personne est victime d'un hameçonnage et communique à un fraudeur des données de sécurité personnalisées (par exemple, son numéro de carte bancaire, la date d'expiration de cette carte, un code réponse/code à usage unique) directement (par exemple par téléphone) ou indirectement (en les renseignant sur un site web vers lequel cette personne a été dirigée au travers d'un hyperlien contenu dans un courriel ou un SMS), les opérations de paiement

[1] Voir aussi HR (Pays-Bas) 21 mai 2021, *TBH* 2022, 169, note R. Steennot; Liège, 9 janvier 2020, *DAOR* 2022, n° 143, 55; J.P. Seraing, 14 juin 2021 (inédit); B. De Waele, "Betwiste online betalingstransacties: analyse van Ombudsfin", *BFR* 2020/bonus, 37. *Autres*: Trib. Bruxelles, 8 janvier 2021, *DAOR* 2022, éd. 141, 102, note D. Blommaert et E. Corthals).

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. Gaat het daarentegen om fraude waarbij de betaler er met een list wordt van overtuigd om zelf de betalingsopdracht te geven, zoals bij factuurfraude, dan betreft het een toegestane betalingstransactie.

Deze verduidelijking strookt met hetgeen door Ombudsfin en in bepaalde rechtspraak wordt aanvaard.

Art. 3

Artikel 74, 1, laatste lid, van de *revised Payment Service directive* (PSD2)[2] biedt in afwijking van de maximale harmonisatie de mogelijkheid om de betaler die grof nalatig is geweest, doch die zelf niet frauduleus heeft gehandeld, noch opzettelijk zijn wettelijke verplichtingen heeft miskend een bijkomende bescherming te bieden, (indien dit geschiedt) rekening houdend met de aard van de persoonlijke beveiligingsgegevens en met de specifieke omstandigheden waarin het betaalinstrument is verloren, gestolen of onrechtmatig is gebruikt.

Gelet op de omvang van de financiële gevolgen die bepaalde betalers hebben ondervonden ingevolge fraude bij op afstand geïnitieerde niet-toegestane elektronische betalingstransacties, vinden wij het gepast om de financiële gevolgen van de betaler ook bij diens grove nalatigheid in te perken. Een grove nalatigheid mag er niet toe leiden dat een betaler het grootste deel van zijn geldmiddelen bij een betalingsdienstaanbieder verloren ziet gaan. Wij hebben daarbij in het bijzonder de situatie voor ogen waarin niet-toegestane betalingstransacties het gevolg zijn van het ontfutselen van de persoonlijke beveiligingsgegevens (zoals bij phishing).

Meer concreet kan de betaler in principe enkel nog aansprakelijk zijn voor de helft van het totale bedrag van de niet-toegestane elektronische betalingstransacties op afstand. Blijkt dit bedrag hoger te zijn dan het bedrag van

[2] 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, bekendgemaakt in het *Publicatieblad van de Europese Unie* van 23 december 2015, L 337/35.

qui en découlent seront réputées non autorisées. Dans ce cas, le payeur n'a en effet pas donné lui-même son consentement à l'exécution de l'ordre de paiement: il n'a pas donné l'ordre de verser un montant donné sur un compte donné (soit l'essence même d'un ordre de paiement). Il s'est uniquement fait soutirer (par exemple, par téléphone ou en ligne) des informations permettant d'effectuer une opération de paiement non autorisée ou d'installer une application de paiement. Une opération de paiement sera en revanche réputée autorisée si la fraude consiste à convaincre par la ruse le payeur de donner lui-même l'ordre de paiement, comme en cas de fraude à la facture.

Cette précision correspond à la distinction qui est admise par Ombudsfin et par certaines décisions judiciaires.

Art. 3

L'article 74, 1, dernier alinéa, de la directive révisée sur les services de paiement (DSP2)[2] prévoit, par dérogation au principe d'harmonisation maximale, la possibilité d'offrir une protection additionnelle au payeur qui a fait preuve de négligence grave mais qui n'a pas agi lui-même de manière frauduleuse ni n'a manqué intentionnellement à ses obligations légales, en tenant compte (dans ce cas) de la nature des données de sécurité personnalisées et des circonstances particulières dans lesquelles l'instrument de paiement a été perdu, volé ou détourné.

Compte tenu de l'ampleur des conséquences financières subies par certains payeurs à la suite d'une fraude impliquant des opérations de paiement électronique initiées à distance et non autorisées, nous estimons qu'il serait également opportun de limiter l'impact financier pour le payeur lorsque celui-ci fait preuve de négligence grave. En effet, une négligence grave ne peut pas avoir pour conséquence de faire perdre à un payeur la majeure partie des fonds qu'il détient auprès d'un prestataire de services de paiement. À cet égard, nous songeons en particulier à la situation dans laquelle des données de sécurité personnalisées sont soutirées pour effectuer des opérations de paiement non autorisées (comme dans le cadre du hameçonnage).

Plus concrètement, la responsabilité du payeur ne pourra en principe plus être engagée qu'à concurrence de la moitié du montant total des opérations de paiement électronique à distance non autorisées. Si ce montant

[2] 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, publiée au *Journal officiel de l'Union européenne* le 23 décembre 2015, L 337/35.

de door de betaler ingestelde uitgavelimieten voor het betaalinstrument, dan wordt de aansprakelijkheid verder beperkt tot dit bedrag. Op die manier wordt vermeden dat de betaler het risico draagt van een aanpassing van de uitgavelimieten door de fraudeur. De betaler kan via de instelling van uitgavelimieten het maximale risico dat hij loopt ook zelf bepalen. Wij zijn er ons van bewust dat deze wetswijziging tot gevolg kan hebben dat het wijzigen van limieten aan bijkomende voorwaarden zal worden onderworpen, doch is van oordeel dat dit gerechtvaardigd is gelet op de grote financiële risico's die betalers anders dreigen te lopen.

Deze beperkingen mogen evenwel niet gelden indien de betaler zijn geheime code, die het betaalinstrument beveiligt, heeft gecommuniceerd. De communicatie van de geheime code vormt een dermate zware nalatigheid dat aansprakelijkheidsbeperkingen niet gerechtvaardigd zijn. In dit kader wordt het onderscheid benadrukt tussen de geheime code en op grond van de geheime code gegenereerde persoonlijke beveiligingsgegevens (bijvoorbeeld *response code* of *onetime password*). Ook voor transacties die plaatsvinden na het ogenblik waarop de betaler kennis had moeten geven (i.e. onverwijld nadat hij zich rekenschap geeft van het onrechtmatig gebruik), gelden de beperkingen niet. De betalingsdienstaanbieder mag geen gevolgen ondervinden van transacties die na dat tijdstip plaatsvinden. Eens de betaler de fraude heeft ontdekt, is hij het best geplaatst om verdere fraude te vermijden.

Benadrukt wordt nog dat het risico van de betaler beperkt blijft tot 50 euro indien geen grove nalatigheid kan worden bewezen, alsook dat de betaler geen enkel risico draagt indien hij de fraude niet kon vaststellen. Deze bepalingen blijven hun relevantie behouden in geval van phishing. Er moet steeds worden nagegaan of de betaler de fraude kon ontdekken en in bevestigend geval of er al dan niet sprake was van grove nalatigheid. Nieuw is "enkel" dat ook in geval van grove nalatigheid de aansprakelijkheid in principe wordt beperkt.

Art. 4

Dit artikel bepaalt de inwerkingtreding. Aan de betalingsdienstaanbieders wordt een periode van ruim drie maanden geboden om de nodige maatregelen te nemen.

Vincent Van Quickenborne (Open Vld)

est supérieur au montant des plafonds de dépenses fixés par le payeur pour l'instrument de paiement, sa responsabilité sera limitée au montant de ces plafonds. On évitera ainsi que le payeur assume le risque d'une modification des plafonds de dépenses par le fraudeur. En fixant des plafonds de dépenses, le payeur pourra aussi déterminer lui-même le risque maximal qu'il assume. Nous sommes conscients du fait que cela pourrait avoir pour conséquence que la modification desdits plafonds soit subordonnée à des conditions supplémentaires, mais nous estimons que les risques financiers majeurs auxquels les payeurs seraient exposés si l'on ne prend pas cette mesure le justifient.

Ces limitations ne pourront toutefois pas s'appliquer si le payeur a communiqué son code secret, qui sécurise l'instrument de paiement. En effet, la communication du code secret constitue une négligence tellement grave qu'il serait injustifié de prévoir des limitations de la responsabilité dans ce cas. Nous soulignons à cet égard la distinction entre le code secret et les données de sécurité personnalisées générées au moyen de ce code (par exemple, un code réponse ou un code à usage unique). Ces limitations ne s'appliqueront pas non plus aux opérations intervenues après le moment où le payeur aurait dû notifier le détournement de son instrument de paiement (c'est-à-dire dès qu'il en a eu connaissance). En effet, les prestataires de services de paiement ne peuvent pas subir les conséquences d'opérations qui interviendraient après ce moment. Dès que le payeur a découvert la fraude, il est le mieux à même de prévenir toute nouvelle fraude.

Nous soulignons encore que le risque supporté par le payeur restera limité à 50 euros si aucune négligence grave ne peut être prouvée. Par ailleurs, le payeur ne courra aucun risque s'il n'était pas en mesure de constater la fraude. Ces dispositions demeurent pertinentes dans le cas du hameçonnage. Il faudra toujours établir si le payeur pouvait découvrir la fraude et, dans l'affirmative, s'il a fait preuve ou non de négligence grave. La "seule" nouveauté est que sa responsabilité sera en principe également limitée en cas de négligence grave.

Art. 4

Cet article règle l'entrée en vigueur. Nous accordons aux prestataires de services de paiement une période d'un peu plus de trois mois pour prendre les mesures nécessaires.

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, laatstelijk gewijzigd door de wet van 19 juli 2018, wordt het woord “zelf” ingevoegd tussen het woord “betaler” en de woorden “heeft ingestemd”.

Art. 3

Artikel VII.44, § 1, van hetzelfde Wetboek, laatstelijk gewijzigd door de wet van 19 juli 2018, wordt aangevuld met een vijfde lid, luidende:

“In afwijking van het vorige lid, is, voor niet-toegestane elektronische betalingstransactie op afstand, de aansprakelijkheid van de betaler, die met grove nalatigheid de hem door artikel VII.38 opgelegde verplichtingen heeft miskend, beperkt tot de helft van het bedrag van die niet-toegestane betalingstransacties, of indien dit bedrag lager is, het bedrag van de voorafgaandelijk aan de fraude door de betaler ingestelde limieten voor het betrokken elektronisch betaalinstrument. Deze beperkingen gelden niet indien de betaler zijn geheime code heeft meegedeeld, noch voor transacties die hebben plaatsgevonden nadat de betaler overeenkomstig artikel VII.38 § 1, 2°, kennis had moeten geven van het onrechtmatige gebruik van zijn betaalinstrument.”

Art. 4

Deze wet treedt in werking op de eerste dag van de derde maand na die waarin ze is bekendgemaakt in het *Belgisch Staatsblad*.

Deze wet is slechts van toepassing op niet-toegestane betalingstransacties die plaatsvinden vanaf de datum van inwerkingtreding van deze wet.

13 november 2024

Vincent Van Quickenborne (Open Vld)

PROPOSITION DE LOI

Article 1er

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

Art. 2

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

Art. 3

L’article VII.44, § 1er, du même Code, modifié en dernier lieu par la loi du 19 juillet 2018, est complété par un alinéa 5 rédigé comme suit:

“Par dérogation à l’alinéa précédent, en ce qui concerne les opérations de paiement électronique à distance non autorisées, la responsabilité du payeur qui a méconnu, à la suite d’une négligence grave, les obligations qui lui sont imposées par l’article VII.38 est limitée à la moitié du montant de ces opérations, ou au montant des plafonds que le payeur a fixés préalablement à la fraude pour l’instrument de paiement électronique concerné si ce montant est plus faible. Ces limites ne s’appliquent pas si le payeur a communiqué son code secret ni lorsqu’il s’agit d’opérations intervenues après que le payeur aurait dû notifier le détournement de son instrument de paiement en application de l’article VII.38 § 1er, 2°.”

Art. 4

La présente loi entre en vigueur le premier jour du troisième mois suivant celui de sa publication au *Moniteur belge*.

Elle s’applique uniquement aux opérations de paiement non autorisées intervenues à compter de sa date d’entrée en vigueur.

13 novembre 2024

Centrale drukkerij - Imprimerie centrale