DOC 56 **0197/001**

BELGISCHE KAMER VAN VOLKSVERTEGENWOORDIGERS

BUITENGEWONE ZITTING 2024

6 september 2024

VOORSTEL VAN RESOLUTIE

betreffende internetfraude

(ingediend door de heer Steven Matheï en mevrouw Leentje Grillaert)

CHAMBRE DES REPRÉSENTANTS DE BELGIQUE

SESSION EXTRAORDINAIRE 2024

6 septembre 2024

PROPOSITION DE RÉSOLUTION

relative à la fraude sur internet

(déposée par M. Steven Matheï et Mme Leentje Grillaert)

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,

Dit voorstel neemt, met wijzigingen, de tekst over van het voorstel DOC 55 2270/001.

De toegenomen digitalisering en connectiviteit is wereldwijd en België kan en mag niet achterblijven. Deze digitalisering biedt niet alleen kansen, maar zorgt ook voor uitdagingen en maakt de samenleving kwetsbaarder voor cyberaanvallen. Internetfraude is de laatste jaren aan een sterke opmars bezig. Fraudeurs maken misbruik van de versnelde digitalisering om zoveel mogelijk geld bij nietsvermoedende personen te ontfutselen.

Internetfraude bestaat uit veel verschillende vormen waaronder *phishing*, vriendschapsfraude, fraude via geldezels, *whaling*, frauduleuze advertenties op sociale media, frauduleuze kredietaanbiedingen, fraude met cryptomunten, beleggingsfraude, valse incassobureaus en frauduleuze webshops.

Bij *phishing* proberen oplichters hun slachtoffers te laten klikken op een link of het downloaden van een app door zich voor te doen als iemand anders bijvoorbeeld de bank, postbedrijf of overheidsdienst. Het doel is om te hengelen of "*phishen*" naar persoonlijke gegevens zoals bankcodes. Eenmaal ze die in hun bezit hebben, kunnen ze in naam van het slachtoffer transacties uitvoeren en gaan ze aan de haal met een hoop geld. In 2023 heeft ongeveer 55 % van de bevolking minstens één phishingbericht ontvangen en werden er bijna 10 miljoen berichten door particulieren gemeld terwijl in 2022 dat er 6 miljoen waren. In 2023 kon men voor ongeveer 40 miljoen euro buit maken door *phishing*.[1] Dit bedrag is de effectief geleden schade dat niet meer terug te vorderen was door de banken.

Bij vriendschapsfraude gebruiken oplichters vaak een vals profiel of gestolen identiteit en gaan ze op zoek naar kwetsbare personen die op zoek zijn naar vriendschap of een partner. Eenmaal ze het vertrouwen gewonnen hebben van het slachtoffer proberen ze geld te ontfutselen. Ook deze vorm van fraude neemt fors toe. In 2021 werden 1.826 meldingen gedaan tegenover 718 meldingen in 2019. De slachtoffers werden het meest benaderd via een datingsite, via sociale media (bijvoorbeeld Facebook), via chat of op een andere

[1] Vr. en Antw. Kamer, Vr. nr. 194, 21 februari 2021 (L. DIERICK).

DÉVELOPPEMENTS

MESDAMES, MESSIEURS,

La présente proposition reprend, en l'adaptant, le texte de la proposition DOC 55 2270/001.

La numérisation et la connectivité accrues sont mondiales et la Belgique ne peut et ne doit pas rester à la traîne. Cette numérisation n'offre pas seulement des opportunités, elle crée aussi des défis et rend la société plus vulnérable aux cyberattaques. Ces dernières années, on observe une nette augmentation de la fraude sur internet. Les fraudeurs profitent de l'accélération de la numérisation pour soutirer un maximum d'argent à des personnes qui ne se doutent de rien.

La fraude sur internet peut prendre de très nombreuses formes, comme le hameçonnage (*phishing*), la fraude à l'amitié, la fraude utilisant des mules bancaires, la fraude au président (*whaling*), les publicités frauduleuses publiées sur les réseaux sociaux, les offres de crédit frauduleuses, les fraudes impliquant des cryptomonnaies, les faux bureaux de recouvrement et les boutiques en ligne frauduleuses.

Dans le cadre d'un hameçonnage, les escrocs tentent de convaincre leurs victimes de cliquer sur un lien ou de télécharger une application en se faisant passer pour une banque, une entreprise postale ou un service public, par exemple, l'objectif étant d'hameçonner des informations personnelles comme des codes bancaires. Une fois ces informations en leur possession, les escrocs peuvent effectuer des transactions au nom de la victime et lui soutirer beaucoup d'argent. En 2023, environ 55 % de la population a reçu au moins un message de *phishing* et près de 10 millions de messages ont été signalés par des particuliers, contre 6 millions en 2022. En 2023, environ 40 millions d'euros pourraient être dérobés par le biais du *phishing*.[1] Ce montant correspond au préjudice effectivement subi qui n'a pas pu être recouvré par les banques.

Dans le cadre de la fraude à l'amitié, les escrocs utilisent souvent un faux profil ou une identité usurpée et ciblent des personnes fragiles qui cherchent à se faire des amis ou à rencontrer un partenaire. Une fois qu'ils ont gagné la confiance de leur victime, ils tentent de lui soutirer de l'argent. Cette forme de fraude est également en plein essor. En 2021, 1.826 signalements ont été effectus, contre 718 en 2019. La majorité du temps, les victimes ont été approchées sur un site de rencontre, sur un réseau social (par exemple, Facebook), sur un site

[1] Questions et réponses, Chambre, Question n° 194, 21 février 2021 (L. DIERICK).

manier. De totale financiële schade bedraagt meer dan 9 miljoen euro en de gemiddelde schade is 17.277 euro. Wel worden de bedragen niet steeds vermeld bij het indienen van een klacht.

Bij het fenomeen van zogenaamde geldezels wordt de bankrekening van een nietsvermoedende burger gebruikt om crimineel geld door te sluizen. Criminelen maken gebruik van geldezels om gestolen geld wit te wassen zonder zelf in beeld te komen. Geldezels beseffen niet altijd dat ze strafbare feiten plegen.

Het zijn voornamelijk jongeren die vatbaar zijn voor deze vorm van fraude. Uit onderzoek van Febelfin in 2019 blijkt dat één op tien jongeren bereid is zijn of haar bankrekening ter beschikking te stellen in ruil voor geld. Vijf procent van de jongeren zou ooit al benaderd geweest zijn om als zogenaamde geldezel te fungeren. Ook lokale politiezones maken melding van een grote stijging van het aantal meldingen en pv's van burgers die als geldezel werden gebruikt.

Een andere vorm van internetfraude is "*whaling*". Dit is een soort van emotionele fraude waarbij oplichters misbruik maken van het gebrek aan fysieke contacten met vrienden of familie. De oplichters stellen een valse vraag om hulp, zogezegd van een vriend of familielid in nood, met als doel om zoveel mogelijk geld te laten overschrijven op hun rekening. Andere vormen van internetfraude zijn frauduleuze advertenties op sociale media en frauduleuze kredietaanbiedingen. Oplichters proberen via frauduleuze advertenties op sociale media en tweedehandswebsites mensen geld af te troggelen. In 2021 werden 773 meldingen ontvangen over frauduleuze advertenties. In 2019 waren dat er 182.[2] Ook uit het jaarverslag van Ombudsfin van 2023 blijkt dat een toenemend aantal fraudegevallen zich situeerde in het kader van een aan- of verkoop via tweedehandsverkoopplatformen zoals Vinted, *2dehands.be* en Facebook Marketplace. Oplichters werken ook vaak met frauduleuze kredietaanbiedingen om aan mensen ongevraagd zeer gunstige kredieten aan te bieden. Zij proberen mensen te lokken met advertenties over kredieten tegen bijzonder gunstige voorwaarden. Om het vertrouwen te winnen, doen ze zich voor als kredietgever of medewerker van een kredietinstelling. Als men hierop ingaat, moeten eerst een aantal fictieve kosten worden betaald en verdwijnt daarna de zogenaamde kredietgever met de noorderzon. Sinds 2016 wordt een toename vastgesteld van het aantal meldingen. Deze toename is niet volledig te wijten aan een toename van het aantal frauduleuze kredietaanbiedingen, maar is ook gedeeltelijk toe te schrijven aan het feit dat meer consumenten de reflex hebben

[2] *Vr. en* Antw. Kamer, Vr. nr. 808, 10 maart 2022 (L. DIERICK).

de *chat* ou d'une autre manière. Le préjudice financier total dépasse les 9 millions d'euros et le préjudice moyen est de 17.277 euros. Cependant, les montants ne sont pas toujours mentionnés lors du dépôt d'une plainte.

Dans le cadre du recours à des "mules bancaires", le compte bancaire d'un citoyen qui ne soupçonne rien est utilisé pour faire transiter de l'argent sale. Les criminels utilisent des mules bancaires pour blanchir de l'argent volé sans que leur nom n'apparaisse. Les mules bancaires ne sont pas toujours conscientes qu'elles commettent des infractions pénales.

Ce sont surtout les jeunes qui peuvent être victimes de ce type de fraude. Selon une étude menée par Febelfin en 2019, un jeune sur dix serait prêt à prêter son compte bancaire contre de l'argent. Cinq pour cent des jeunes auraient déjà été approchés pour servir de «mule bancaire». Et les zones de police locales font également état d'une forte augmentation du nombre de signalements et de procès-verbaux de citoyens ayant joué le rôle de mule bancaire.

Une autre forme de fraude sur internet est le "*whaling*". Il s'agit d'une sorte d'escroquerie jouant sur l'émotion: les escrocs profitent du manque de contacts physiques avec les amis ou la famille. Ils envoient une fausse demande d'aide qui provient prétendument d'un ami ou d'un membre de la famille en difficulté. L'unique but de cette démarche est de faire verser un maximum d'argent sur leur compte. Parmi les autres formes de fraude sur internet figurent les publicités frauduleuses sur les réseaux sociaux et les offres de crédit frauduleuses. Les escrocs tentent de soutirer de l'argent à leurs victimes par le biais d'annonces frauduleuses sur les réseaux sociaux et les sites de vente de seconde main. En 2021, 773 signalements ont été reçus concernant des publicités frauduleuses. En 2019, on en a enregistré 182.[2] Le rapport annuel 2023 de l'Ombudsfin montre également qu'un nombre croissant de cas de fraude ont eu lieu dans le cadre d'un achat ou d'une vente via des plateformes de vente d'occasion telles que Vinted, *2dehands.be* et Facebook Marketplace. Les escrocs proposent aussi souvent des offres de crédit frauduleuses visant à fournir aux personnes ciblées un crédit non sollicité et très favorable. Ils tentent de les attirer par des annonces de prêts à des conditions particulièrement favorables. Pour gagner leur confiance, ils se font passer pour des prêteurs ou des collaborateurs d'un établissement de crédit. Lorsqu'une victime réagit à l'annonce, il lui faut d'abord payer un certain nombre de frais fictifs, puis le prétendu prêteur disparaît dans la nature. Depuis 2016, une augmentation du nombre de signalements a été observée. Cette augmentation n'est pas entièrement

[2] *Q. et R.* Chambre, Q. n° 808, 10 mars 2022 (L. DIERICK).

om zich tot de FSMA en FOD Economie te wenden. In 2021 heeft de FOD Economie 227 meldingen ontvangen over frauduleuze kredietaanbiedingen tegenover 125 meldingen in 2019. De FSMA heeft 245 meldingen ontvangen in 2021.[3]

Bij beleggingsfraude worden consumenten aangezet om te investeren in een bedrieglijke belegging. De aanbieder van de belegging is geen gereguleerde aanbieder, maar een frauduleus *tradingplatform*. De belegging wordt niet terugbetaald en de belegger verliest zijn inleg. In haar jaarverslag meldt de FSMA dat het aantal klachten over beleggingsfraude sterk toeneemt. In 2023 heeft de FSMA een recordaantal klachten ontvangen van consumenten en publiceerde waarschuwingen voor 146 frauduleuze *online-tradingplatformen* die actief zijn op de Belgische markt.[4]

Andere vormen van internetfraude zijn onder meer fraude met cryptomunten, valse incassobureaus en frauduleuze webshops. De afgelopen jaren ligt het aantal meldingen van frauduleuze webshops hoog. Terwijl in 2019 er 6.706 meldingen waren, waren er in 2020 maar liefst 11.628 meldingen over frauduleuze webshops en in 2022 waren er 8.586. Aangezien het steeds moeilijker wordt voor de consument om malafide webshops te herkennen, moet het bestrijden en sluiten van malafide webshops een prioriteit worden. Naast sensibilisering is het daarbij ook belangrijk dat de Economische Inspectie sneller malafide webshops kan opsporen en sluiten.[5]

Sensibilisering en educatie

Inzetten op sensibilisering is de beste strategie om consumenten te beschermen tegen internetfraude. Het is belangrijk dat burgers preventief worden gewaarschuwd voor de verschillende vormen van internetfraude. Wie waakzamer is en internetfraude kan herkennen, zal minder vaak in de val van de fraudeurs trappen.

De FOD Economie voert regelmatig sensibiliseringscampagnes om consumenten te waarschuwen. Zo liep in 2020-2021 de campagne “trap niet in de val.” De website “*temooiomwaartezijn.be*” bevat als campagnesite informatie over fraude met cryptomunten,

[3] *Vr. en Antw.* Kamer, Vr. nr. 807, 10 maart 2022 (L. DIERICK).
[4] FSMA, *Jaarverslag 2024,* p. 43.
[5] Voorstel van resolutie betreffende het bestrijden van malafide webshops, *Parl.St.* Kamer, DOC 55 0084/001.

due à une augmentation du nombre d’offres de crédit frauduleuses, elle s’explique aussi en partie par le fait que davantage de consommateurs ont le réflexe de se tourner vers la FSMA et le SPF Économie. En 2021, le SPF Économie a reçu 227 signalements relatifs à des offres de crédit frauduleuses, contre 125 en 2019. La FSMA a enregistré 245 signalements en 2021.[3]

La fraude à l’investissement consiste à inciter les consommateurs à placer de l’argent dans un investissement frauduleux. Le fournisseur de l’investissement n’est pas un fournisseur réglementé, mais une plateforme de trading frauduleuse. L’investissement n’est pas remboursé et l’investisseur perd son argent. Dans son rapport annuel, la FSMA indique que le nombre de plaintes concernant des cas de fraude à l’investissement est en forte augmentation. En 2023, la FSMA a enregistré un nombre record de plaintes de consommateurs et a émis des avertissements pour 146 plateformes de trading en ligne frauduleuses opérant sur le marché belge.[4]

Parmi les autres formes de fraude sur internet figurent la fraude aux cryptomonnaies, les faux bureaux de recouvrement et les boutiques en ligne frauduleuses. Ces dernières années, le nombre de signalements de boutiques en ligne frauduleuses a été élevé. Alors qu’en 2019, il y a eu 6.706 signalements, en 2020, il y a eu jusqu’à 11.628 signalements de boutiques en ligne frauduleuses et en 2022, il y en a eu 8.586. Les consommateurs éprouvent de plus en plus de difficultés à reconnaître les boutiques en ligne malhonnêtes, si bien que la lutte contre ces dernières et leur fermeture doivent devenir une priorité. Outre la sensibilisation, il est également important que l’Inspection économique puisse détecter et fermer plus rapidement les boutiques en ligne malhonnêtes.[5]

Sensibilisation et éducation

Miser sur la sensibilisation est la meilleure stratégie pour protéger les consommateurs contre la fraude en ligne. Il importe de mettre préventivement en garde les citoyens contre les différentes formes de fraude en ligne. En effet, si les citoyens sont plus vigilants et capables de reconnaître la fraude sur le web, ils risqueront moins de tomber dans les pièges des fraudeurs.

Le SPF Économie mène régulièrement des campagnes de sensibilisation pour mettre en garde les consommateurs. Cela a notamment été le cas en 2020-2021, avec la campagne “Évitez les pièges”. En tant que site de campagne, le site “*tropbeaupouretrevrai.be*” contient

[3] *Q et R.* Chambre, Q. n° 807, 10 mars 2022 (L. DIERICK).
[4] FSMA, *Rapport annuel 2024,* p. 43.
[5] Proposition de résolution relative à la lutte contre les *webshops* malhonnêtes, *Doc. parl.* Chambre, DOC 55 0084/001.

beleggingsfraude en vriendschapsfraude. Daarnaast bestaat de campagnesite "*trapnietindeval.be*" rond drie andere vormen van fraude namelijk valse incassobureaus, frauduleuze webshops en *phishing* met valse personen/organisaties en sinds 2024 is er ten slotte een website "Stop Bedrog" over fraude en oplichterij in het algemeen. Inzake beleggingsfraude publiceert de FSMA regelmatig meldingen over verdachte *tradingplatformen*. De FSMA waarschuwt hiermee consumenten voor onregelmatige activiteiten. Daarnaast informeert, sensibiliseert en waarschuwt ook het Centrum voor Cybersecurity België (CCB) de Belgische bevolking over cybercriminaliteit zoals phishingberichten via de website van Safeonweb. Voor de consument die op zoek is naar informatie kan dit verwarrend zijn, omdat ze naargelang het soort fraude op verschillende websites terechtkomen. Wij zijn dan ook van mening dat er één website moet worden gemaakt rond internetfraude. Die website moet het referentiepunt zijn voor elke burger die wordt geconfronteerd met een vorm van internetfraude. Die website kan ook een directe link bevatten naar *ConsumerConnect*. Naast financiële schade die slachtoffers lijden, mag ook het mentale aspect niet worden vergeten. Slachtoffers die van het ene op het andere moment een grote som geld zijn kwijtgeraakt, schamen zich omdat ze zich hebben laten vangen, zijn angstig en zitten met financiële en emotionele kopzorgen. De website moet dan ook een luik bevatten over een hulpaanbod waar slachtoffers terecht kunnen.

Hoewel onderwijs een bevoegdheid is van de gemeenschappen, heeft de federale overheid ook een rol in de financiële educatie van de bevolking. De FSMA heeft hierin een wettelijke opdracht die zij vervult via allerlei initiatieven zoals "*Wikifin.be*", "Wikifin Lab" en een educatief programma voor jongeren en hun leerkrachten. Ook de Nationale Bank heeft programma's om leerkrachten te ondersteunen in hun economische kennis. Bij al deze initiatieven is het van belang dat ook de opmars van internetfraude, de werkwijze en de economische gevolgen aan bod komen.

Belang van meldingen

Het is belangrijk dat slachtoffers de fraude melden op *ConsumerConnect*. *ConsumerConnect* zorgt ervoor dat meldingen gecentraliseerd worden en laat zo toe om nieuwe vormen van bedrog snel te detecteren, waardoor de bevoegde instantie(s) op een snelle manier de nodige maatregelen, zoals sensibiliseren, kunnen nemen om de praktijk aan te pakken. De melder krijgt onmiddellijk advies op zijn computerscherm te zien over welke

des informations sur les arnaques aux cryptomonnaies, les arnaques à l'investissement et les fraudes à l'amitié. En outre, le site de campagne "*evitezlespieges.be*" a été mis en ligne pour sensibiliser à trois autres formes de fraude, à savoir les fausses agences de recouvrement, les *webshops* frauduleux et le *phishing* impliquant de fausses personnes/organisations et enfin, depuis 2024, il existe un site web "Stop Arnaques" sur la fraude et les escroqueries en général. En ce qui concerne la fraude à l'investissement, la FSMA publie régulièrement des mises en garde concernant des plateformes de trading suspectes. La FSMA met ainsi en garde les consommateurs contre les activités irrégulières. En outre, le Centre pour la Cybersécurité Belgique (CCB) informe, sensibilise et met en garde la population belge contre la cybercriminalité, comme les messages de *phishing* via le site web Safeonweb. Pour les consommateurs à la recherche d'informations, cette multiplicité de ressources peut être déroutante car, selon le type de fraude en ligne, ils aboutissent sur différents sites web s'ils veulent en savoir plus. Nous estimons dès lors qu'un site web unique doit être créé pour traiter de la fraude en ligne. Ce site doit être le point de référence pour tout citoyen confronté à une forme de fraude en ligne et pourrait également proposer un lien direct vers *ConsumerConnect*. Outre le préjudice financier subi par les victimes, il ne faut pas oublier la dimension psychologique. Les victimes qui, du jour au lendemain, ont perdu une grosse somme d'argent ont honte de s'être fait prendre, sont anxieuses et ont des tracas financiers et émotionnels. Le site internet devrait donc inclure un volet dédié aux offres d'aide auxquelles les victimes peuvent s'adresser.

Bien que l'éducation soit une compétence communautaire, le gouvernement fédéral a également un rôle à jouer dans l'éducation financière de la population. La FSMA a une mission légale dans ce domaine, qu'elle remplit par le biais de diverses initiatives telles que "*Wikifin.be*", "Wikifin Lab" et un programme éducatif pour les jeunes et leurs enseignants. La Banque nationale dispose également de programmes visant à soutenir les enseignants dans leurs connaissances économiques. Il importe que toutes ces initiatives abordent également l'essor de la fraude en ligne, ses méthodes et ses conséquences économiques.

Importance des signalements

Il est important que les victimes de fraude fassent une déclaration sur le site *ConsumerConnect*. *ConsumerConnect* assure la centralisation des signalements et permet ainsi de détecter rapidement de nouvelles formes d'escroquerie. L'instance ou les instances compétentes peuvent ainsi prendre rapidement les mesures nécessaires, notamment sur le plan de la sensibilisation, pour lutter contre cette pratique. Le plaignant

stappen hij of zij nog moet ondernemen en wie daarbij kan helpen. De Economische Inspectie kan op basis van deze melding een onderzoek starten of deze melding doorsturen naar de bevoegde inspectiedienst.

Naast het melden van internetfraude is het belangrijk dat het slachtoffer klacht indient bij de lokale politie en snel contact opneemt met de bank zodat de bank de overschrijving kan proberen te onderscheppen of de rekening kan blokkeren.

Verantwoordelijkheid financiële instellingen

In het Wetboek van economisch recht (WER) werd door de omzetting van de PSDII-richtlijn voorzien in aansprakelijkheidsregels van de betalingsdienstaanbieder voor niet-toegestane betalingstransacties. Het is aan de betalingsdienstaanbieder om structuren op te zetten of te organiseren binnen zijn onderneming waardoor betalingstransacties op een veilige manier kunnen plaatsvinden. Er kan van een betaler niet verwacht worden dat hij van dit technisch proces een volledige kennis of overzicht heeft.[6] Artikel VII. 44 WER regelt de mogelijke aansprakelijkheid van de betaler en omvat een uitzondering die in geval van twijfel in het voordeel van de betaler moet worden geïnterpreteerd. De aansprakelijkheid van de betaler is beperkt tot een maximumbedrag van 50 euro. De betaler moet dus enkel het verlies van maximum 50 euro dragen m.b.t. alle niet-toegestane betalingstransacties die voortvloeien uit het gebruik van een verloren of gestolen betaalinstrument of uit onrechtmatig gebruik van een betaalinstrument. De betaler draagt geen enkel verlies indien het verlies, diefstal of onrechtmatig gebruik van een betaalinstrument niet kon worden vastgesteld door de betaler voordat een betaling plaatsvond. De betaler draagt enkel alle verliezen indien hij frauduleus heeft gehandeld of opzettelijk of door grove nalatigheid. De bewijslast inzake bedrog, opzet of grove nalatigheid komt toe aan de betalingsdienstaanbieder.

Uit het jaarverslag van Ombudsfin, de ombudsdienst voor financiële diensten, blijkt ook dat er meer betwistingen zijn tussen banken en burgers over deze mogelijke terugbetaling door de bank na een fraudegeval. Dit komt doordat de vraag of banken al dan niet wettelijk tot tussenkomst in de schade ten gevolge van niet toegestane betalingstransacties gehouden zijn, afhankelijk is van de vraag of de fraude al dan niet op voorhand gedetecteerd kon worden door het slachtoffer en van de beoordeling van een grove nalatigheid in hoofde van het slachtoffer.

[6] Wetsontwerp houdende wijziging en invoering van bepalingen inzake betalingsdiensten in verschillende boeken van het Wetboek van economisch recht, *Parl.St.* Kamer 2017-2018, Doc 54 3131/001.

reçoit immédiatement sur son écran des conseils sur les mesures à prendre et les personnes susceptibles de l'aider. Sur la base de cette notification, l'Inspection économique peut ouvrir une enquête ou transmettre cette notification à l'inspection compétente.

Outre le fait de signaler la fraude dont elle a fait l'objet sur internet, il est important que la victime dépose une plainte auprès de la police locale et prenne rapidement contact avec la banque afin que celle-ci puisse tenter d'intercepter le virement ou de bloquer le compte.

Responsabilité des établissements financiers

Le Code de droit économique (CDE) a prévu, via la transposition de la directive PSDII, des règles de responsabilité incombant au prestataire de services de paiement en ce qui concerne les opérations de paiement non autorisées. Il appartient au prestataire de services de paiement de mettre en place ou d'organiser au sein de son entreprise des structures permettant d'effectuer des opérations de paiement de manière sécurisée. On ne peut attendre d'un payeur qu'il ait une connaissance ou une vue d'ensemble complète de ce processus technique.[6] L'article VII. 44 du CDE règle la question de la responsabilité éventuelle du payeur et contient une exception qui, en cas de doute, doit être interprétée en faveur de celui-ci. La responsabilité du payeur est limitée à un montant maximum de 50 euros. Le payeur doit donc uniquement supporter une perte de 50 euros maximum pour toute opération de paiement non autorisée résultant de l'utilisation d'un instrument de paiement perdu ou volé ou du détournement d'un instrument de paiement. Le payeur ne supporte aucune perte si la perte, le vol ou le détournement d'un instrument de paiement ne pouvait être détecté par le payeur avant le paiement. Le payeur ne supporte la totalité des pertes que s'il a agi frauduleusement, intentionnellement ou par négligence grave. La charge de la preuve en matière de fraude, d'intention ou de négligence grave incombe au prestataire de services de paiement.

Le rapport annuel d'Ombudsfin, le service de médiation des services financiers, montre également qu'il y a davantage de litiges entre les banques et les citoyens à propos de cet éventuel remboursement par la banque après un cas de fraude. La question de savoir si les banques sont légalement tenues ou non d'intervenir dans les préjudices causés par des opérations de paiement non autorisées dépend en effet de la possibilité qu'avait ou non la victime de détecter la fraude à l'avance et de l'appréciation d'une éventuelle négligence grave de sa

[6] Projet de loi portant modification et insertion de dispositions en matière de services de paiement dans différents livres du Code de droit économique, *Doc. parl.*, Chambre 2017-2018, Doc 54 3131/001.

Voor beide beoordelingen dient rekening te worden gehouden met alle feitelijke omstandigheden.

Banken zouden steeds vaker een beroep doen op “grove nalatigheid” waardoor de consument alle verliezen moet dragen. In het jaarverslag van Ombudsfin blijkt dat banken het been vaak stijf houden en het begrip grove nalatigheid ruim interpreteren. Het kan niet de bedoeling zijn dat een kleine onachtzaamheid van de consument door de bank beschouwd wordt als een grove nalatigheid. Deze aansprakelijkheidsregels hebben tot doel om de consument te beschermen en moeten dan ook correct worden toegepast. Het is dus belangrijk dat banken hun verantwoordelijkheid opnemen zoals voorzien in het WER. De resolutie wil dan ook dat de naleving van deze aansprakelijkheid beter wordt gecontroleerd en effectief gesanctioneerd bij overtredingen. Bovendien zijn veel burgers niet of niet goed op de hoogte van hun rechten met betrekking tot een mogelijke terugbetaling door hun bank. Ook stelde Ombudsfin vast dat de fraudedetectiesystemen van de bank hadden tekortgeschoten . Het gevolg is dat in 2023 slechts in 32,7 % de bemiddeling van Ombudsfin in de gegronde dossiers succesvol afgesloten werd met een tussenkomst van de bank. Zo blijkt dat 2 op de 3 slachtoffers zelf moeten opdraaien voor het geld dat ze verliezen aan fraudeurs en amper een derde van de slachtoffers volledig of gedeeltelijk worden terugbetaald door hun bank.

Wanneer een consument een debet- of kredietkaart verliest, moet hij of zij onmiddellijk de uitgever van de kaart, meestal de bank, op de hoogte brengen. Bij verlies of diefstal moet de consument dan ook onmiddellijk naar Card Stop bellen waardoor de kaart onmiddellijk wordt geblokkeerd. Na deze aangifte is de consument in principe dan ook niet langer verantwoordelijk en moet de bank de bedragen terugbetalen.

Ook slachtoffers van internetfraude zouden steeds 24/7 een kennisgeving moeten kunnen doen via het bellen van een algemeen nummer zodat de bank onmiddellijk de rekening of rekeningen kan blokkeren.

Recent heeft elke bank een meldpunt waar slachtoffers 24 op 7 terecht kunnen, maar slachtoffers moeten wel telkens via hun bank nagaan wat het telefoonnummer is binnen de openingsuren en naar welk nummer zij kunnen bellen buiten de openingsuren. Banken zouden altijd beschikbaar moeten zijn om rekeningen te blokkeren en het is belangrijk dat er nog een stap verder wordt gegaan en een algemeen telefoonnummer wordt opgericht, naar analogie met Card Stop.

part. Pour établir ces deux appréciations, toutes les circonstances factuelles doivent être prises en compte.

Les banques invoqueraient de plus en plus souvent la “négligence grave”, laissant ainsi le consommateur supporter la totalité des pertes. Le rapport annuel de l’Ombudsfin montre que les banques gardent souvent les pieds sur terre et interprètent la notion de négligence grave de manière large. Il serait inacceptable qu’une petite inattention du consommateur soit considérée par la banque comme une négligence grave. Le but de ces règles de responsabilité est de protéger le consommateur, et elles doivent donc être appliquées correctement. Il est dès lors important que les banques assument leurs responsabilités comme le prévoit le CDE. C’est pourquoi nous demandons que le respect de cette responsabilité soit mieux contrôlé et que les violations de ces règles soient effectivement sanctionnées. En outre, de nombreux citoyens ne connaissent pas ou pas suffisamment leurs droits en ce qui concerne les possibilités de remboursement de leurs pertes par leur banque. L’Ombudsfin a également constaté que les systèmes de détection des fraudes de la banque étaient défaillants. En conséquence, en 2023, seulement 32,7 % des médiations de l’Ombudsfin dans des cas avérés ont été conclues avec succès par une intervention de la banque. Cela montre que 2 victimes sur 3 doivent payer elles-mêmes l’argent qu’elles ont perdu au profit des fraudeurs et qu’à peine un tiers des victimes sont totalement ou partiellement remboursées par leur banque.

Lorsqu’un consommateur perd une carte de débit ou de crédit, il doit immédiatement en informer l’émetteur de la carte, généralement la banque. En cas de perte ou de vol, le consommateur doit aussi immédiatement appeler Card Stop, qui bloquera aussitôt la carte. Après cette déclaration, le consommateur n’est en principe plus responsable et la banque doit rembourser les montants perdus.

Les victimes de fraude sur internet devraient également pouvoir faire une déclaration 24 heures sur 24 et 7 jours sur 7 en appelant un numéro général afin que la banque puisse immédiatement bloquer le ou les comptes.

Récemment, toutes les banques ont mis en place une hotline à laquelle les victimes peuvent s’adresser 24 heures sur 24 et 7 jours sur 7, mais les victimes doivent à chaque fois vérifier auprès de leur banque quel est le numéro de téléphone pendant les heures d’ouverture et quel est le numéro qu’elles peuvent appeler en dehors des heures d’ouverture. Les banques devraient toujours être disponibles pour bloquer les comptes et il est important d’aller plus loin et d’établir un numéro de téléphone général, à l’instar de Card Stop.

Banken moeten ervoor zorgen dat hun klanten, zowel burgers als ondernemers, altijd veilig kunnen internetbankieren. Ze moeten dan ook meer en sneller investeren in beveiliging.

Ten slotte moeten banken zo snel mogelijk een IBAN-naamcontrole invoeren. In mei 2022 heeft de Belgische banksector aangekondigd om na Nederland en het Verenigd Koninkrijk ook in België de IBAN-naamcontrole uit te werken, maar momenteel is dit nog niet van toepassing. Met de IBAN-naamcontrole controleren banken tijdens een overschrijvingsopdracht of het rekeningnummer en de naam van de begunstigde overeenstemmen om zo bepaalde vormen van fraude met overschrijvingen, in het bijzonder factuurfraude, in te dijken.

Uitwisseling informatie

Een goede uitwisseling van informatie tussen de financiële instellingen onderling en tussen de financiële instellingen en de overheid is belangrijk om internetfraude tegen te gaan. Het uitwisselen van gegevens biedt meer kansen aan de financiële instellingen om criminele netwerken te ontdekken en om preventieve acties uit te voeren.

Binnen het bestaande wettelijk kader is er recent een anti-witwasplatform opgestart tussen Febelfin, Assuralia en de federale overheid met het oog om op een efficiënte en veilige manier informatie uit te wisselen die nuttig kan zijn voor de doeltreffende en passende uitvoering van de wettelijke taken van alle deelnemers.

Het publiek-privaat platform is er in eerste instantie op gericht om de strijd tegen witwassen gezamenlijk aan te pakken met zo veel mogelijk betrokken partijen. De opstart van dit platform moet financiële instellingen er ook toe aanzetten om sneller bankrekeningen te kunnen blokkeren, waarmee verdachte betalingen worden uitgevoerd.

Opsporing en vervolging

Uiteraard worden ook de politiediensten geconfronteerd met een stijgend aantal klachten met betrekking tot internetfraude. Waar er in 2016 op jaarbasis nog 13.045 feiten in de Algemene Nationale Gegevensbank (ANG) werden genoteerd, waren er dat in de eerste drie trimesters van 2020 al 24.375. Toch blijft dit voor de politiediensten een relatief nieuw fenomeen en bestaan er ook bij hen nog steeds onduidelijkheden hieromtrent. Daarom is het noodzakelijk om proactief de verschillende vormen van internetfraude te communiceren aan de lokale politiezones zodanig dat zij in staat zijn om burgers te waarschuwen voor de gevaren van internetfraude

Les banques doivent veiller à ce que leurs clients, qu'il s'agisse de citoyens ou d'entrepreneurs, puissent toujours accéder aux services bancaires en ligne en toute sécurité. Elles doivent donc investir davantage et plus rapidement dans la sécurité.

Enfin, les banques devraient introduire le contrôle des noms IBAN dès que possible. En mai 2022, le secteur bancaire belge a annoncé qu'après les Pays-Bas et le Royaume-Uni, le contrôle du nom IBAN serait également mis en place en Belgique, mais ce n'est pas encore le cas actuellement. Avec le contrôle du nom IBAN, les banques vérifient si le numéro de compte et le nom du bénéficiaire correspondent lors d'un ordre de virement afin de lutter contre certains types de fraude au virement, en particulier la fraude à la facture.

Échange d'informations

Un bon échange d'informations entre les institutions financières et entre les institutions financières et les autorités publiques est important pour lutter contre la fraude sur le web. L'échange de données offre aux institutions financières davantage de possibilités de dépister les réseaux criminels et de mener des actions préventives.

Dans le cadre légal existant, une plateforme de lutte contre le blanchiment a récemment été mise en place entre Febelfin, Assuralia et les autorités fédérales en vue de permettre un échange utile et sécurisé des informations pouvant être utiles à l'exécution efficace et appropriée des tâches légales de tous les participants.

La plateforme publique-privée doit d'abord permettre de lutter conjointement contre le blanchiment d'argent en impliquant un maximum de parties prenantes. La mise en place de cette plateforme doit également inciter les institutions financières à bloquer plus rapidement les comptes bancaires utilisés pour effectuer des paiements suspects.

Recherche et poursuites

Les forces de police sont naturellement aussi confrontées à un nombre croissant de plaintes contre la fraude sur le web. Alors qu'en 2016, 13.045 faits étaient enregistrés dans la Banque de données nationale générale (BNG), on en comptait déjà 24.375 au cours des trois premiers trimestres de 2020. Toutefois, ce phénomène reste relativement neuf pour les services de police, et des incertitudes subsistent à ce sujet, même à leur niveau. Il convient dès lors de communiquer de manière proactive les différentes formes de fraude sur le web aux zones de police locales afin qu'elles soient en mesure d'avertir les citoyens des dangers de la fraude sur le web et de

en om hen te begeleiden in geval dat zij het slachtoffer geworden zijn van enige vorm van internetfraude. Het is eveneens aangewezen om de politiediensten te betrekken bij een geïntegreerde aanpak van internetfraude zodanig dat zij ook hun steentje kunnen bijdragen in het opzetten van preventieve acties samen met de andere betrokken actoren.

Volgens ministeriële richtlijn COL 2/2002 tot regeling van de taakverdeling, samenwerking, coördinatie en integratie tussen de lokale en de federale politie inzake de opdrachten van gerechtelijke politie is internetfraude in de eerste plaats een taak van de lokale politie. Toch lijkt op het terrein onduidelijkheid te zijn ontstaan met betrekking tot deze taakverdeling. Lokale politiekorpsen verwijzen immers naar de federale politie om gevolg te kunnen geven aan een aangifte van internetfraude. Hierdoor ontstaat het risico dat bij slachtoffers het gevoel gaat ontstaan dat er geen of te weinig gevolg gegeven wordt aan hun aangifte. Het is daarom noodzakelijk om de lokale politiekorpsen beter te informeren over de problematiek van internetfraude en over de afhandeling van aangiftes van dergelijke misdrijven. De taakverdeling tussen de lokale en federale politiediensten moet daarbij voldoende duidelijk zijn. Het voorstel van resolutie vraagt dan ook om de informatie-uitwisseling tussen de lokale en de federale politie verder te versterken en de taakverdeling indien nodig verder te verduidelijken.

Zoals reeds eerder aangegeven is de zorg en ondersteuning van slachtoffers van internetfraude enorm belangrijk. Artikel 46 van de Wet op het Politieambt schrijft voor dat de politiediensten personen die hulp of bijstand behoeven in contact brengen met de gespecialiseerde diensten. Om de politiediensten de kans te geven zich ook met betrekking tot internetfraude van deze taak te kunnen kwijten, dienen zij in voldoende mate opgeleid en geïnformeerd te zijn over de verschillende kanalen, waarbij slachtoffers van internetfraude terecht kunnen en waarnaar zij slachtoffers kunnen doorverwijzen.

Vandaag wordt reeds voorzien in basis- en voortgezette opleidingen voor bepaalde beroepscategorieën die in aanraking komen met internetfraude. Zo bevat de basisopleiding voor inspecteur bij de Geïntegreerde Politie reeds een specifieke cursus inzake de materies aangaande cybercriminaliteit en voorziet de politie in een aanbod van een dertigtal voortgezette opleidingen betreffende cybercriminaliteit die door elke politieagent gevolgd kunnen worden. De doelstelling van dit voorstel van resolutie is om de regering te vragen die inspanningen voor alle betrokken sectoren verder te zetten en waar nodig ook uit te breiden.

leur fournir un accompagnement au cas où ils seraient victimes d'une forme quelconque de fraude de cette nature. Il s'indique également d'associer les forces de police à une lutte intégrée contre la fraude sur le web afin qu'elles puissent également jouer leur rôle dans la mise en place d'actions préventives avec les autres acteurs concernés.

Selon la directive ministérielle COL 2/2002 organisant la répartition des tâches, la collaboration, la coordination et l'intégration entre la police locale et la police fédérale en ce qui concerne les missions de police judiciaire, la lutte contre la fraude sur internet est avant tout une mission de la police locale. Cependant, une certaine confusion semble être apparue sur le terrain en ce qui concerne cette répartition des tâches. Les corps de police locaux renvoient en effet à la police fédérale pour pouvoir donner suite à un signalement de fraude sur internet, avec le risque que les victimes aient le sentiment que l'on ne donne pas suffisamment, voire pas du tout suite à leur déclaration. Il est donc nécessaire de mieux informer les corps de police locaux sur la problématique relative à la fraude sur internet et sur le traitement des déclarations de ces infractions. La répartition des tâches entre les services de police locaux et fédéraux doit être suffisamment claire à cet égard. La proposition de résolution appelle donc à renforcer l'échange d'informations entre la police locale et la police fédérale et à clarifier davantage la répartition des tâches si nécessaire.

Comme indiqué ci-dessus, la prise en charge et le soutien des victimes de la fraude sur internet revêtent une importance considérable. L'article 46 de la loi sur la fonction de police dispose que les services de police doivent mettre les personnes ayant besoin d'aide ou d'assistance en contact avec les services spécialisés. Pour permettre aux services de police de s'acquitter de leur tâche également en ce qui concerne la fraude sur internet, il convient de les former et informer suffisamment sur les différents canaux auxquels les victimes de la fraude sur internet peuvent s'adresser et vers lesquels ils peuvent aiguiller ces victimes.

Aujourd'hui, des formations de base et avancées sont déjà prévues pour certaines catégories professionnelles en contact avec la cyberfraude. Par exemple, la formation de base d'inspecteur de la police intégrée comprend déjà un cours spécifique sur les questions liées à la cybercriminalité, et la police propose une trentaine de formations continues sur la cybercriminalité qui peuvent être suivies par n'importe quel policier. L'objectif de cette proposition de résolution est de demander au gouvernement de poursuivre et, le cas échéant, d'étendre ces efforts à tous les secteurs concernés.

Om de problematiek van de internetfraude adequaat en effectief te kunnen aanpakken, is het noodzakelijk om een goed zicht te hebben op de grootteorde van de problematiek. Dit voorstel van resolutie beoogt de beeldvorming met betrekking tot internetfraude te verbeteren. Het Nationaal Veiligheidsplan 2022-2025 omschrijft daartoe een aantal cruciale acties waarnaar in dit verzoek verwezen wordt. Met een "barrièremodel" wordt gedoeld op een methodiek waarmee men zicht krijgt op een gans crimineel fenomeen of proces door de verschillende stappen die criminelen zetten om delicten te plegen in kaart te brengen en waaruit verschillende mogelijkheden van aanpak voor de politie en haar partners kunnen worden afgeleid.

Voorts startte de federale politie in juni 2022 een campagne om gespecialiseerde hoofdinspecteurs aan te werven en om zo personeel met voldoende expertise aan te trekken. Voldoende expertise op alle niveaus binnen de Geïntegreerde Politie is cruciaal om een adequaat beeld te krijgen van de omvang van de problematiek van de internetfraude. Voorliggend verzoek spoort de regering dan ook aan de geleverde inspanningen verder te zetten.

Momenteel laten de registraties in de ANG niet toe om binnen de categorie internetfraude een onderscheid te maken naargelang het gaat om feiten met betrekking tot vriendschapsfraude, identiteitsfraude of enige andere vorm van internetfraude. Internetfraude omvat in de ANG vandaag alle vormen van oplichting die via het internet zijn gepleegd. Dit maakt het moeilijker om de verschillende vormen van internetfraude correct in kaart te brengen. Het zou daarom goed zijn om ook in de ANG een onderverdeling mogelijk te maken die gelijkaardig is aan degene die gehanteerd wordt door de FOD Economie, zodanig dat de mogelijkheid ontstaat om binnen de categorie internetfraude wel degelijk een onderscheid tussen de verschillende fenomenen te maken.

Bij het in kaart brengen van de verschillende vormen van internetfraude is het eveneens belangrijk om de politiediensten te betrekken bij een te organiseren structureel overleg met de financiële instellingen, parketten en de telecomoperatoren waarin de problematiek van internetfraude besproken en in kaart gebracht wordt en waaruit eventuele oplossingen voor de problematiek kunnen voortvloeien. Daarnaast dienen politiediensten en magistraten voldoende opgeleid te worden met betrekking tot dit fenomeen.

Pour s'attaquer de manière adéquate et efficace à la question de la fraude sur Internet, il est nécessaire d'avoir une vision claire de l'ampleur du problème. Cette proposition de résolution vise à améliorer la perception de la fraude sur Internet. À cette fin, le plan national de sécurité 2022-2025 définit un certain nombre d'actions cruciales mentionnées dans la présente demande. Un "modèle de barrière" est une méthodologie qui permet de comprendre l'ensemble d'un phénomène ou d'un processus criminel en cartographiant les différentes étapes suivies par les criminels pour commettre des délits et à partir desquelles diverses options d'approche pour la police et ses partenaires peuvent être déduites.

En outre, en juin 2022, la police fédérale a lancé une campagne de recrutement d'inspecteurs en chef spécialisés afin d'attirer du personnel disposant d'une expertise suffisante.Une expertise suffisante à tous les niveaux au sein de la police intégrée est cruciale pour obtenir une image adéquate de l'étendue du problème de la fraude sur Internet. La présente demande encourage donc le gouvernement à poursuivre les efforts entrepris.

Actuellement, les enregistrements dans la BNG ne permettent pas de faire, au sein de la catégorie de la fraude sur internet, une distinction selon qu'il s'agit d'actes liés à la fraude à l'amitié, à la fraude à l'identité ou à toute autre forme de fraude sur internet. La fraude sur internet comprend aujourd'hui dans la BNG toutes les formes de fraude commises par le biais d'internet. Il est donc compliqué de cartographier correctement les différentes formes de fraude sur internet. Il serait par conséquent utile de créer, dans la BNG, une subdivision similaire à celle utilisée par le SPF Économie, afin de pouvoir distinguer les différents phénomènes au sein de la catégorie de la fraude sur internet.

Dans le cadre de la cartographie des différentes formes de fraude sur internet, il importe également d'associer les services de police à une concertation structurelle à organiser avec les institutions financières, les parquets et les opérateurs de télécommunications, dans le cadre de laquelle le problème de la fraude sur internet sera discuté et analysé, et d'où pourront émerger des solutions possibles au problème. Par ailleurs, les services de police et les magistrats doivent recevoir une formation adéquate à propos de ce phénomène.

Tenslotte dienen ook de strafbaarstellingen van naderbij bekeken te worden, teneinde na te gaan of zij voldoende adequaat zijn om de verschillende vormen van internetfraude te bestraffen.

Steven Matheï (cd&v)
Leentje Grillaert (cd&v)

Enfin, il convient également d'examiner les incriminations de plus près afin de vérifier si elles sont suffisamment appropriées pour sanctionner les différentes formes de fraude sur internet.

VOORSTEL VAN RESOLUTIE

De Kamer van volksvertegenwoordigers,

A. gelet op de sterke opmars van internetfraude;

B. opmerkend dat er veel verschillende vormen van internetfraude bestaan;

C. overwegende dat het inzetten op sensibilisering de beste strategie is om consumenten te beschermen tegen internetfraude;

D. gelet op het belang van het melden van internet-fraude;

E. gelet op de vaststellingen van Ombudsfin, zoals weergegeven in haar jaarverslag van 2020;

F. vaststellend dat een goede uitwisseling van informatie tussen de financiële instellingen onderling en tussen de financiële instellingen en de overheid nodig is om internetfraude tegen te gaan;

G. gelet op de nood aan opsporing en vervolging van internetfraude;

H. overwegende dat de Europese instellingen zich ook steeds meer zorgen maken over internetfraude en het bestrijden daarvan als gerechtvaardigd belang erkennen;

I. overwegende dat de Kadernota Integrale Veiligheid (KIV) 2022-2025 digitale veiligheid beschouwt als een huidig en toekomstig veiligheidsfenomeen en daartoe onder de noemer “Aanpak van het misbruik van persoonlijke gegevens” verschillende actiepunten definieert, bijvoorbeeld inzake sensibilisering, kennisoverdracht, internationale samenwerking en het blokkeren van frauduleuze berichten;

J. overwegende dat in het Nationaal Veiligheidsplan (NVP) 2022-2025 “internet en de nieuwe technologieën” één van de vier transversale thema’s is waarvoor vernieuwing noodzakelijk is en waarvoor programma’s uitgewerkt zullen worden met een geheel aan samenhangende projecten en acties die inzetten op nieuwe politionele ontwikkelingen en dat hacking, informaticasabotage, informaticabedrog en oplichtingen met internet in het NVP 2022-2025 als prioritair veiligheidsfenomeen worden beschouwd;

PROPOSITION DE RÉSOLUTION

La Chambre des représentants,

A. considérant que la fraude sur internet est un fléau de plus en plus répandu;

B. considérant qu’il existe de nombreuses formes de fraude sur internet;

C. considérant que la sensibilisation est le meilleur moyen de protéger les consommateurs contre ce phénomène;

D. considérant qu’il est important de signaler la fraude sur internet;

E. vu les constatations d’Ombudsfin exposées dans son rapport annuel 2020;

F. considérant qu’il est nécessaire d’organiser un bon échange d’informations entre les établissements financiers et entre ceux-ci et les pouvoirs publics pour lutter contre la fraude sur internet;

G. considérant qu’il est capital de détecter la fraude sur internet et d’en poursuivre les auteurs;

H. considérant que les institutions européennes sont, elles aussi, de plus en plus préoccupées par la fraude sur internet et qu’elles reconnaissent qu’il se justifie de lutter contre ce phénomène;

I. considérant que le mémorandum-cadre sur la sécurité intégrale 2022-2025 considère la sécurité numérique comme un phénomène de sécurité actuel et futur et, à cette fin, définit plusieurs points d’action sous le titre “Lutter contre l’utilisation abusive des données à caractère personnel”, par exemple en matière de sensibilisation, de transfert de connaissances, de coopération internationale et de blocage des messages frauduleux;

J. considérant que, dans le plan national de sécurité (PNS) 2022-2025, “l’internet et les nouvelles technologies” est l’un des quatre thèmes transversaux pour lesquels l’innovation est nécessaire et pour lesquels des programmes seront élaborés avec un ensemble de projets et d’actions cohérents qui tireront parti des nouveaux développements policiers, et considérant que le piratage, le sabotage informatique, la fraude informatique et les escroqueries sur l’internet sont considérés comme un phénomène de sécurité prioritaire dans le PNS 2022-2025;

K. gelet op artikel 6 van verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG;

VERZOEKT DE FEDERALE REGERING:

1. nieuwe sensibiliseringscampagnes uit te werken om burgers preventief te waarschuwen voor internetfraude, te helpen om fraude te herkennen, aan te zetten om waakzamer te zijn om niet in de val te trappen en om hen aan te sporen om fraude te melden en zich te informeren welke stappen ze moeten ondernemen;

2. één website uit te bouwen en te communiceren als referentiepunt rond internetfraude, waar alle verschillende vormen van internetfraude aan bod komen, waarop staat welke stappen slachtoffers kunnen nemen en waar slachtoffers de fraude ook kunnen melden en waarop een overzicht van het hulpaanbod voor slachtoffers staat;

3. geïntegreerde aanpak van internetfraude door een werkgroep op te richten, waar onder meer de FOD Economie, Febelfin, FSMA, Centrum voor Cybersecurity (CCB), telecomoperatoren en de politie deel van uitmaken, om gezamenlijke preventieve acties te organiseren;

4. om over de verschillende vormen van internetfraude te communiceren met lokale politiezones en gemeentes, zodat zij op hun beurt meer kennis kunnen verzamelen en burgers kunnen waarschuwen en begeleiden;

5. structureel overleg te organiseren met de financiële instellingen, maar ook met de politie, het parket en de telecomoperatoren in dit land, teneinde dit probleem in kaart te brengen en mogelijke oplossingen te bespreken;

6. om een algemeen telefoonnummer op te richten, naar analogie met Card Stop, waar slachtoffers van internetfraude bij vermoeden van fraude onmiddellijk naar kunnen bellen dat 24 op 24u, 7 dagen op 7 bereikbaar is, om tijdelijk hun rekening(en) te laten blokkeren door de bank en waarbij banken nadien instaan voor de nazorg om de rekening terug te deblokkeren;

7. de banksector aan te sporen om snel de IBAN-naamcontrole in te voeren om bepaalde vormen van fraude met overschrijvingen, in het bijzonder factuurfraude, in te dijken;

K. vu l'article 6 du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE;

DEMANDE AU GOUVERNEMENT FÉDÉRAL:

1. d'élaborer de nouvelles campagnes de sensibilisation afin de mettre les citoyens en garde contre la fraude sur internet, de les aider à reconnaître cette fraude, de les inciter à être plus vigilants pour éviter de tomber dans le piège et de les encourager à signaler les fraudes et à s'informer sur les démarches à entreprendre;

2. de créer un site internet unique appelé à devenir le point de référence dans le domaine de la fraude sur internet, qui abordera les différentes formes de fraude sur internet et expliquera quelles sont les démarches pouvant être entreprises par les victimes, sur lequel les victimes pourront signaler la fraude et qui offrira un aperçu de l'aide disponible pour les victimes;

3. d'adopter une approche intégrée de la fraude sur internet en créant un groupe de travail composé notamment de représentants du SPF Économie, de Febelfin, de la FSMA, du Centre pour la Cybersécurité Belgique (CCB), des opérateurs de télécommunications et de la police, dans le but d'organiser des actions préventives communes;

4. de communiquer sur les différentes formes de fraude sur internet avec les zones de police locale et avec les communes, afin que celles-ci puissent acquérir davantage de connaissances et avertir et accompagner les citoyens;

5. d'organiser une concertation structurelle avec les établissements financiers, mais aussi avec la police, le ministère public et les opérateurs de télécommunications de ce pays, afin d'identifier ce problème et de discuter des solutions possibles;

6. de mettre en place, par analogie avec Card Stop, un numéro de téléphone général que les victimes de fraude sur internet pourront immédiatement appeler en cas de suspicion de fraude et qui sera accessible 24 heures sur 24, 7 jours sur 7, afin de faire bloquer temporairement leur(s) compte(s) par la banque, les banques assurant ensuite le suivi pour débloquer le compte;

7. d'exhorter le secteur bancaire à introduire rapidement la vérification du nom IBAN afin de réduire certaines formes de fraude par virement, en particulier la fraude à la facture;

8. bekendheid te verhogen van de huidige aansprakelijkheidsregels, zoals voorzien in artikel VII.43 en artikel VII.44 van het Wetboek van economisch recht, om de consumentenbescherming te verhogen, aangezien veel consument niet op de hoogte zijn van hun rechten;

9. beter te controleren op de naleving en daadwerkelijk te sanctioneren bij overtreding van de aansprakelijkheidsregels die worden toegepast door betalingsdienstaanbieders in artikel VII.43 en artikel VII.44 van het Wetboek van economisch recht, en daarbij te onderzoeken om het sanctiesysteem, zoals toegepast door de Economische Inspectie, te wijzigen, zodat zij zelf ook administratieve boetes kunnen opleggen aan betalingsdienstaanbieders;

10. blijvend te voorzien in voldoende basis- en voortgezette opleidingen voor mensen die professioneel in aanraking komen met de problematiek van internetfraude, zoals bankbedienden, politieagenten en magistraten;

11. de informatie-uitwisseling tussen de lokale en de federale politie met betrekking tot de problematiek van internetfraude en de afhandeling van aangiftes dienaangaande verder te versterken en de taakverdeling tussen de federale en de lokale politie indien nodig verder te verduidelijken;

12. de beeldvorming met betrekking tot het fenomeen internetfraude en de informatiepositie van de Geïntegreerde politie dienaangaande te verbeteren door:

12.1. in de Algemene Nationale Gegevensbank van de politie een onderverdeling te maken die gelijkaardig is aan deze gehanteerd binnen de FOD Economie, door binnen de categorie internetfraude een onderscheid tussen de verschillende fenomenen van deze problematiek te maken zodanig dat de verschillende vormen van internetfraude correct in kaart kunnen worden gebracht;

12.2. overeenkomstig het Nationaal Veiligheidsplan 2022-2025, ernaar te streven alle beschikbare informatie, zoals bijvoorbeeld deze van het meldpunt van de FOD Economie, te integreren in de politionele informatiebronnen;

12.3. overeenkomstig het Nationaal Veiligheidsplan 2022-2025, een beschrijving van het crimineel proces met betrekking tot het fenomeen internetfraude uit te werken aan de hand van een zogenaamd “barrièremodel”;

12.4. op alle niveaus binnen de politie de gepaste expertise en capaciteit op te bouwen in het kader van de strijd tegen internetfraude en daartoe de ingezette

8. de veiller à améliorer la diffusion des règles actuelles de responsabilité telles que prévues par les articles VII.43 et VII.44 du Code de droit économique afin de renforcer la protection des consommateurs, car beaucoup d’entre eux ne connaissent pas leurs droits;

9. de mieux contrôler le respect et de sanctionner réellement les violations des règles de responsabilité qui sont appliquées par les prestataires de services de paiement en vertu des articles VII.43 et VII.44 du Code de droit économique, et d’examiner à cet égard la possibilité de modifier le système de sanction appliqué par l’Inspection économique de manière à ce qu’elle puisse également infliger elle-même des amendes administratives aux prestataires de services de paiement;

10. de continuer à prévoir une formation de base et avancée suffisante aux personnes qui sont en contact professionnel avec les questions de fraude sur Internet, telles que les employés de banque, les officiers de police et les magistrats;

11. de renforcer encore l’échange d’informations entre la police locale et la police fédérale en ce qui concerne le problème de la fraude sur Internet et le traitement des rapports y afférents, et de clarifier davantage la répartition des tâches entre la police fédérale et la police locale si nécessaire;

12. d’améliorer la perception du phénomène de la fraude sur Internet et la position d’information de la police intégrée à cet égard:

12.1. en créant dans la base de données nationale générale de la police une subdivision similaire à celle utilisée au sein du SPF Économie, en distinguant au sein de la catégorie de la fraude sur Internet les différents phénomènes de cette problématique, de sorte que les différentes formes de fraude sur Internet puissent être correctement cartographiées;

12.2. conformément au Plan national de sécurité 2022-2025, s’efforcer d’intégrer toutes les informations disponibles, telles que celles de la hotline du SPF Économie, dans les sources d’information de la police;

12.3. conformément au Plan national de sécurité 2022-2025, élaborer une description du processus criminel lié au phénomène de la fraude sur l’internet à l’aide d’un modèle dit “à barrières”;

12.4. développer l’expertise et les apacités appropriées à tous les niveaux au sein de la police dans le cadre de la lutte contre la fraude sur Internet et, à cette fin,

inspanningen inzake de rekrutering van gespecialiseerde hoofdinspecteurs verder te zetten;

13. in de gegevensbank van het College van Procureurs-generaal een onderverdeling te maken die gelijkaardig is aan deze gehanteerd binnen de FOD Economie, door binnen de categorie internetfraude een onderscheid te maken tussen de zaken met betrekking tot vriendschapsfraude en andere zaken met betrekking tot informaticafraude of misbruik van vertrouwen om op die manier dit fenomeen correct in kaart te brengen;

14. te onderzoeken of er, rekening houdend met de wettelijke bepalingen inzake beroepsgeheim en de verwerking van persoonsgegevens, al dan niet dossierspecifieke data gedeeld kan worden tussen financiële instellingen en de overheid;

15. te onderzoeken of de huidige strafbaarstellingen voldoende accuraat zijn om het fenomeen van internetfraude en de verschillende vormen hiervan adequaat te vervolgen en bestraffen;

16. de samenwerking in de strijd tegen internetfraude met de verschillende betrokken actoren op Europees en internationaal niveau verder te zetten en waar mogelijk uit te breiden.

29 augustus 2024

Steven Matheï (cd&v)
Leentje Grillaert (cd&v)

poursuivre les efforts initiés concernant le recrutement d'inspecteurs en chef spécialisés;

13. d'opérer dans la banque de données du Collège des procureurs généraux une subdivision similaire à celle qui est utilisée au sein du SPF Économie, en opérant une distinction dans la catégorie fraude sur internet entre les affaires concernant la fraude à l'amitié et d'autres affaires concernant la fraude informatique ou l'abus de confiance de manière à inventorier correctement ce phénomène;

14. d'examiner si, compte tenu des dispositions légales en matière de secret professionnel et de traitement des données à caractère personnel, des données spécifiques au dossier peuvent être partagées ou non entre les institutions financières et les pouvoirs publics;

15. d'examiner si les incriminations actuelles sont suffisamment précises afin de poursuivre et de sanctionner adéquatement le phénomène de la fraude sur internet et ses différentes formes;

16. poursuivre et, si possible, développer la coopération dans la lutte contre la fraude sur Internet avec les différents acteurs impliqués au niveau européen et international.

29 août 2024

Centrale drukkerij - Imprimerie centrale