

CHAMBRE DES REPRÉSENTANTS
DE BELGIQUE

3 juin 2021

PROPOSITION DE RÉSOLUTION

**relative à la lutte contre la cyberfraude
utilisant des mules bancaires**

(déposée par
MM. Michael Freilich et Joy Donné)

BELGISCHE KAMER VAN
VOLKSVERTEGENWOORDIGERS

3 juni 2021

VOORSTEL VAN RESOLUTIE

**betreffende het bestrijden van
cyberfraude via geldezel**

(ingedien door
de heren Michael Freilich en Joy Donné)

04759

N-VA	: <i>Nieuw-Vlaamse Alliantie</i>
Ecolo-Groen	: <i>Ecologistes Confédérés pour l'organisation de luttes originales – Groen</i>
PS	: <i>Parti Socialiste</i>
VB	: <i>Vlaams Belang</i>
MR	: <i>Mouvement Réformateur</i>
CD&V	: <i>Christen-Démocratique en Vlaams</i>
PVDA-PTB	: <i>Partij van de Arbeid van België – Parti du Travail de Belgique</i>
Open Vld	: <i>Open Vlaamse liberalen en democraten</i>
Vooruit	: <i>Vooruit</i>
cdH	: <i>centre démocrate Humaniste</i>
DéFI	: <i>Démocrate Fédéraliste Indépendant</i>
INDEP-ONAFH	: <i>Indépendant - Onafhankelijk</i>

<i>Abréviations dans la numérotation des publications:</i>		<i>Afkorting bij de numering van de publicaties:</i>	
DOC 55 0000/000	<i>Document de la 55^e législature, suivi du numéro de base et numéro de suivi</i>	DOC 55 0000/000	<i>Parlementair document van de 55^e zittingsperiode + basisnummer en volgnummer</i>
QRVA	<i>Questions et Réponses écrites</i>	QRVA	<i>Schriftelijke Vragen en Antwoorden</i>
CRIV	<i>Version provisoire du Compte Rendu Intégral</i>	CRIV	<i>Voorlopige versie van het Integraal Verslag</i>
CRABV	<i>Compte Rendu Analytique</i>	CRABV	<i>Beknopt Verslag</i>
CRIV	<i>Compte Rendu Intégral, avec, à gauche, le compte rendu intégral et, à droite, le compte rendu analytique traduit des interventions (avec les annexes)</i>	CRIV	<i>Integraal Verslag, met links het deft nitieve integraal verslag en rechts het vertaald beknopt verslag van de toespraken (met de bijlagen)</i>
PLEN	<i>Séance plénière</i>	PLEN	<i>Plenum</i>
COM	<i>Réunion de commission</i>	COM	<i>Commissievergadering</i>
MOT	<i>Motions déposées en conclusion d'interpellations (papier beige)</i>	MOT	<i>Moties tot besluit van interpellaties (beige kleurig papier)</i>

DÉVELOPPEMENTS

MESDAMES, MESSIEURS,

La cybercriminalité a connu une croissance exponentielle en 2020. Plus concrètement, la *Computer Emergency Response Team* (CERT) belge avait déjà recueilli 5 387 signalements en septembre 2020, ce qui était déjà supérieur au nombre total des signalements de 2019 (4 484). Une des formes les plus fréquentes de fraude en ligne est l'hameçonnage (*phishing*). Celui-ci consiste à envoyer de faux courriels dans le but de s'emparer de données de manière à pouvoir dérober de l'argent. Le mode opératoire des criminels est très professionnel, si bien qu'il est difficile de déceler la supercherie à première vue. Un lien est souvent disponible vers un faux site web imitant celui d'une banque, par exemple, qui ressemble parfaitement à la version originale grâce à l'utilisation de la présentation et des logos originaux. Dès qu'un paiement y est effectué au moyen d'un mot de passe ou d'une carte bancaire, les criminels peuvent faire un usage malveillant des données et voler de l'argent. D'autres méthodes sont également parfois utilisées pour tromper les gens, via le téléphone, de faux SMS (*smishing*) ou d'autres ruses.

Le point commun de toutes ces formes d'escroquerie est qu'elles visent à extorquer de l'argent. Les escrocs font appel à des "mules bancaires" ou "*money mules*" afin de ne pas se faire prendre eux-mêmes en faisant verser l'argent directement sur leur propre compte, par exemple. Ces mules sont des personnes qui, contre rémunération, prêtent leur compte bancaire et/ou leur carte bancaire ainsi que leur code pin. L'argent volé peut ainsi être dépensé en ligne, être transféré sur un autre compte bancaire en Belgique ou à l'étranger ou être retiré à un distributeur de billets.

Les mules bancaires proviennent souvent de groupes vulnérables en proie à des problèmes financiers. Les étudiants qui ne peuvent plus travailler en raison de la fermeture du secteur horeca sont également à la recherche d'un revenu complémentaire. Aussi sont-ils prêts, conscients ou non de la gravité de l'infraction, à se rendre complices de cette forme d'escroquerie. Suivant une procédure caractéristique, les malfaiteurs les contactent dans la vie réelle ou en ligne en leur promettant de gagner rapidement de l'argent. Les mules sont abordées à proximité des gares ou dans des parcs, mais les prises de contact sont de moins en moins physiques en raison de la distanciation sociale imposée par la pandémie. La plupart des contacts ont lieu en ligne. À cet égard des réseaux sociaux comme Instagram, WhatsApp, Telegram et Snapchat sont très utilisés au même titre que de fausses offres d'emploi.

TOELICHTING

DAMES EN HEREN,

Cybercriminaliteit kende in 2020 een exponentiële groei. In september 2020 ging het meer bepaald al om 5 387 meldingen bij het Belgische *Computer Emergency Response Team* (CERT), wat reeds meer is dan het totaal aantal meldingen in 2019 (4 484 meldingen). Een van de meest voorkomende vormen van onlinefraude is *phishing*. Daarbij worden valse e-mails verstuurd met als doel gegevens te bemachtigen om zo geld te kunnen ontvreemden. De criminelen gaan daarbij zeer professioneel te werk, waardoor de valsheid op het eerste gezicht moeilijk te achterhalen is. Vaak is er een link naar een nagemaakte website van bijvoorbeeld een bank, die er door het gebruik van de originele logo's en lay-out exact uitziet zoals de originele versie. Van zodra daar dan een betaling uitgevoerd wordt met een wachtwoord of bankkaart, kunnen de criminelen de gegevens misbruiken en geld stelen. Soms worden mensen ook op andere manieren om de tuin geleid, via de telefoon, via valse sms'en (*smishing*) of door middel van andere gewiekste trucs.

Wat al die vormen van oplichting gemeen hebben, is dat zij de bedoeling hebben om mensen geld afhandig te maken. Om zelf niet betrapt te worden, bijvoorbeeld door het geld rechtstreeks op hun eigen rekening te laten overschrijven, gebruiken de oplichters zogenaamde "geldezels" of "*money mules*". Dat zijn mensen die tegen een vergoeding hun bankrekening en/of bankkaart met pincode uittellen. Het gestolen geld kan zo online uitgegeven worden, naar een andere bankrekening in binnen- of buitenland worden doorgestuurd of aan een bankautomaat worden afgehaald.

Vaak komen de geldezels uit kwetsbare groepen die met financiële problemen kampen. Ook studenten, die door de sluiting van de horecasector hun studentenjob niet meer kunnen uitoefenen, zijn op zoek naar een bijverdienste. Daardoor zijn ze bereid om, zich al dan niet bewust van de ernst van het misdrijf, mee te helpen aan deze vorm van oplichting. Via een herkenbaar patroon worden ze in het echte leven of online gecontacteerd met de belofte om snel geld te verdienen. Mensen worden aangeklampt in stationsbuurten of parken, maar de benadering gebeurt door de beperkte sociale contacten ten gevolge van de pandemie steeds minder fysiek. Het merendeel van de contacten vindt digitaal plaats. Daarbij wordt veel gebruik gemaakt van sociale media zoals Instagram, WhatsApp, Telegram en Snapchat, maar ook van valse jobadvertenties.

Les intéressés ont l'impression de rendre un service qui ne demande guère d'efforts alors qu'en réalité, ils aident des criminels à écouter de l'argent volé. En outre, les véritables auteurs effacent toute trace permettant de les identifier grâce à cette construction financière. En fait, la mule bancaire fait la sale besogne et a de fortes chances de se faire prendre en raison de la grande vigilance du secteur bancaire. Contrairement à ce qui lui semble, la mule bancaire commet toutefois bien une infraction en ce qu'elle se rend complice d'un blanchiment d'argent dont elle peut être tenue responsable. Qui plus est, il s'agit rarement d'une transaction unique, la mule entrant ainsi dans un cercle vicieux. Dès qu'une personne a joué une fois le rôle de mule bancaire, les criminels attendent qu'elle le fasse de plus en plus souvent et n'hésitent pas à recourir aux menaces et à la violence physique pour la convaincre.

En dépit de risques importants, le phénomène des mules bancaires est en plein essor. Par exemple, le 16 avril 2021, le quotidien *Het Nieuwsblad* a publié une interview d'une mule bancaire condamnée pour avoir mis son compte à la disposition de cybercriminels. De plus, ces agissements sont sanctionnés par de fortes amendes et par des peines d'emprisonnement pouvant aller jusqu'à un an. Mais le cas précité n'en fut qu'un parmi d'autres. Par ailleurs, toute mule bancaire condamnée risque d'être inscrite sur la liste noire de sa banque, cette inscription pouvant fortement compliquer l'ouverture d'un compte ou la souscription d'un emprunt.

Les banques sont de plus en plus conscientes de ce problème et organisent dès lors régulièrement des campagnes de dissuasion. Febelfin a par exemple fait appel à l'actrice populaire Liandra Sadzo pour mettre en ligne une vidéo qui vise tout particulièrement les jeunes insuffisamment conscients des risques que prend la mule bancaire. Ce n'est que lorsque son compte a été bloqué par sa banque et que sa "personne de contact" s'est complètement volatilisée que la mule bancaire commence à comprendre dans quel pétrin elle s'est mise. De plus, les mules bancaires mineures risquent de mettre également leurs parents en difficulté car ils sont responsables des actes de leurs enfants.

Le problème majeur de cette construction financière est que, souvent, seule la mule bancaire peut être identifiée et condamnée. Étant donné que, dans notre pays, les banques ne disposent pas réellement de moyens pour attaquer le mal à la racine, les véritables criminels restent hors de portée de la justice et de la police et ils peuvent continuer à chercher de nouvelles victimes en toute impunité. En effet, les institutions financières ne peuvent souvent rien faire d'autre que bloquer le compte bancaire sur lequel elles observent des transactions ou des paiements suspects. Pour pouvoir démanteler les

Het lijkt alsof men voor een kleine moeite een vriendendienst levert, terwijl men in werkelijkheid criminelen helpt om gestolen geld te versluizen. Bovendien wissen de echte daders door deze financiële constructie elk spoor naar zichzelf uit. De geldezel knapt in feite het vuile werk op en loopt door de grote pakkans vanwege de banksector een hoog risico om tegen de lamp te lopen. Hoewel het lijkt alsof men niets strafbaars doet, is dat het wel degelijk het geval, aangezien men zich medeplichtig maakt aan het witwassen van geld waarvoor men aansprakelijk kan worden gesteld. Daarenboven blijft het zelden bij één transactie, waardoor er een vicieuze cirkel ontstaat. Van zodra men één keer voor geldezel gespeeld heeft, verwachten criminelen dit steeds vaker en deinzen ze er niet voor terug om bedreigingen en fysiek geweld te gebruiken om die persoon te overtuigen.

Ondanks het grote gevaar is het fenomeen van de *money mules* aan een opmars bezig. Op 16 april 2021 verscheen er bijvoorbeeld in de krant *Het Nieuwsblad* een interview met een geldezel die zijn rekening had laten gebruiken door internetfraudeurs en daarom veroordeeld werd. Daarbij worden er hoge geldboetes en gevangenisstraffen tot een jaar uitgesproken. Dit is slechts één van de vele schrijnende verhalen. Bovendien riskeren veroordeelde *money mules* op een zwarte lijst bij hun bank terecht te komen, waardoor zij veel moeilijker een rekening kunnen openen of een lening kunnen afsluiten.

De banken zelf zijn zich ook meer en meer bewust geworden van dit probleem en organiseren daarom op regelmatige basis ontradingscampagnes. Zo heeft Febelfin een filmpje gelanceerd met de populaire actrice Liandra Sadza, dat speciaal is gericht op jongeren die zich niet genoeg bewust zijn van het gevaar om voor geldezel te spelen. Pas als hun rekening geblokkeerd is door de bank en hun "contactpersoon" compleet van de wereld is verdwenen, begint het te dagen in wat voor hel ze zijn beland. Daarenboven dreigen ze, als ze minderjarig zijn, hun ouders hierin mee te sleuren aangezien die voor hen verantwoordelijk zijn.

Het grote probleem met deze financiële constructie is dat vaak enkel de geldezel gevatten kan worden en als enige veroordeeld wordt. De echte criminelen blijven buiten schot voor het gerecht en de politie en kunnen ongehinderd nieuwe slachtoffers blijven zoeken. Dat komt doordat het in ons land de banken aan echte middelen ontbreekt om het probleem aan de bron te bestrijden. Financiële instellingen kunnen namelijk vaak slechts de bankrekening blokkeren waarop zij verdachte betalingen of transacties waarnemen. Er is veel meer nood aan uitwisseling van gegevens tussen banken om criminelle

réseaux criminels, les échanges de données entre les banques devraient être beaucoup plus nombreux. Or, les banques ne peuvent pas officiellement communiquer entre elles au sujet des transactions suspectes, car la législation visant la lutte contre le blanchiment ne contient aucune disposition prévoyant l'échange de données entre les institutions financières.

Il convient en outre de tenir compte des règles strictes du règlement général sur la protection des données (RGPD) en vigueur depuis 2018. En effet, ces règles assurent la protection des données personnelles au sein de l'Union européenne et prévoient que ces données ne peuvent être traitées qu'à condition qu'un motif de traitement valable justifie leur traitement. Le RGPD prévoit six motifs de traitement. Dans ce cadre, les plus pertinents sont le consentement, l'obligation légale et l'intérêt légitime. Bien entendu, en cas de suspicion de fraude, il ne convient nullement de d'abord demander au suspect d'autoriser le traitement des données. La lutte contre la fraude est généralement admise comme un intérêt légitime en application du RGPD, mais les banques peuvent être réticentes à invoquer cet argument juridique pour échanger des informations à propos de transactions suspectes, car toutes les transactions suspectes ne se révèlent pas frauduleuses ultérieurement. La crainte de lourdes amendes infligées en application du RGPD et les éventuelles atteintes à la réputation n'y sont certainement pas étrangères. Par conséquent, il semble qu'il ne soit actuellement possible d'améliorer l'échange d'informations à propos des transactions suspectes entre les banques qu'en prévoyant un cadre juridique.

La présente proposition de résolution vise dès lors à souligner la nécessité d'une modification de la loi en ce sens et à appeler le gouvernement à élaborer rapidement et adéquatement une législation *ad hoc*. Aux Pays-Bas, il existe depuis longtemps un système de prévention des risques (*Risk Warning System*) qui permet aux banques d'entamer des enquêtes entre elles en cas de blanchiment d'argent. Nous demandons dès lors au gouvernement de prévoir un système similaire en Belgique. Il est urgent de mettre un terme au blanchiment d'argent imputable aux mules bancaires. Il n'est pas acceptable de permettre à des criminels de continuer à agir sans être inquiétés et de laisser des jeunes gens ainsi détruire leur vie. Il s'agit d'énormes sommes d'argent sale canalisées quotidiennement et sur lesquelles la société ne pourra avoir aucune prise tant que nous n'agirons pas. Les règles relatives au respect de la vie privée ne doivent en outre pas empêcher de légiférer. Nous appelons donc les ministres compétents à prendre contact avec leurs homologues néerlandais pour savoir comment nous pouvons mettre en place un système efficace.

netwerken te kunnen oprollen. Officieel is er echter geen communicatie tussen banken over verdachte transacties mogelijk: de antiwitwaswetgeving bevat geen bepalingen die in een gegevensuitwisseling tussen verschillende financiële instellingen voorzien.

Daarnaast moet ook rekening worden gehouden met de strenge regels van de Algemene Verordening Gegevensbescherming (AVG), die sinds 2018 van kracht zijn. Die regels waarborgen namelijk de bescherming van de persoonsgegevens binnen de Europese Unie en bepalen dat zij enkel verwerkt mogen worden mits er een geldige verwerkingsgrond is. Er zijn zes verwerkingsgronden onder de AVG, waarvan toestemming, wettelijke verplichting en gerechtvaardigd belang de meest relevante in dit kader zijn. Uiteraard is het totaal onwenselijk om bij een vermoeden van fraude vooraf toestemming aan een verdachte te vragen. Bestrijding van fraude wordt algemeen aanvaard als een gerechtvaardigd belang in het kader van de AVG, maar wellicht deinden de banken er voor terug om die rechtsgrond in te roepen om informatie over verdachte transacties uit te wisselen, omdat niet iedere verdachte transactie naderhand frauduleus blijkt te zijn. De vrees voor zware boetes in het kader van de AVG en eventuele reputatieschade zal daar niet vreemd aan zijn. Bijgevolg lijkt een betere informatie-uitwisseling over verdachte transacties tussen de banken op heden slechts mogelijk door te voorzien in een wettelijk kader.

In dit voorstel van resolutie willen wij dan ook de noodzaak van een dergelijke wetswijziging benadrukken en de regering ertoe oproepen om snel en adequaat werk te maken van gepaste wetgeving. In Nederland is er sinds lang een *Risk Warning System*, dat de banken ertoe in staat stelt om onderling onderzoeken te starten bij het witwassen van geld. Wij vragen daarom aan de regering om een gelijkaardig systeem voor België in het leven te roepen. Er moet dringend paal en perk worden gesteld aan het witwassen via geldezels. Het is niet aanvaardbaar dat wij criminelen ongestoord verder laten opereren en daarbij jonge mensen hun leven laten verwoesten. Het gaat om enorme bedragen aan criminelen geld die dagelijks versluisd worden en waar de samenleving geen vat op kan krijgen als wij niets ondernemen. Privacyregels mogen daarbij niet verhindren dat regelgeving uitgevaardigd wordt. Wij roepen de bevoegde ministers op om contact op te nemen met de Nederlandse collega's om te leren hoe wij een effectief systeem kunnen implementeren.

De plus, les institutions européennes sont également de plus en plus conscientes du problème des mules bancaires et de la difficulté d'appréhender les criminels qui se cachent derrière elles.¹ Compte tenu de cet intérêt manifesté au niveau européen, le moment est à présent venu d'agir.

De Europese instellingen zijn zich ook meer en meer bewust geraakt van het probleem van de *money mules* en de moeilijkheid om de criminelen erachter te vatten.¹ In het licht van deze klaarblijkelijke aandacht op Europees niveau is het momentum aanwezig om nu actie te ondernemen.

Michael FREILICH (N-VA)
Joy DONNÉ (N-VA)

¹ Voir, par exemple, la communication conjointe au Parlement européen et au Conseil "Résilience, dissuasion et défense: doter l'UE d'une cybersécurité solide" du 13 juillet 2017, <https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:52017JC0450&from=EN>, et "Europol spoort duizenden 'geldezel's' op bij witwasonderzoek" in *Europa Nu*, 2 décembre 2020, https://www.europa-nu.nl/id/vle9kgqd4kzs/nieuws/europol_spoort_duizenden_geldezel_s_op?ctx=vh6ukzb3nnt0.

¹ Zie bijvoorbeeld de Gezamenlijke Mededeling van de Europese Commissie aan het Europees Parlement en de Raad "Weerbaarheid, afschrikking en defensie: bouwen aan sterke cyberbeveiliging voor de EU" van 13 juli 2017, <https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:52017JC0450&from=EN>, en "Europol spoort duizenden 'geldezel's' op bij witwasonderzoek" in *Europa Nu*, 2 december 2020, https://www.europa-nu.nl/id/vle9kgqd4kzs/nieuws/europol_spoort_duizenden_geldezel_s_op?ctx=vh6ukzb3nnt0.

PROPOSITION DE RÉSOLUTION

LA CHAMBRE DES REPRÉSENTANTS,

A. vu la croissance exponentielle de la cybercriminalité observée ces dernières années;

B. considérant que les criminels ont souvent recours à des "mules bancaires" pour transférer sur d'autres comptes bancaires, afin de rester invisibles, l'argent qu'ils ont soutiré à leurs victimes par le biais de pratiques frauduleuses;

C. considérant que les "mules bancaires" s'exposent au risque d'être condamnées, mais aussi au risque de figurer sur la liste noire d'une banque, cette inscription pouvant les empêcher ultérieurement d'ouvrir un compte courant ou d'obtenir un prêt;

D. considérant qu'il apparaît que les mules bancaires sont souvent de jeunes individus insuffisamment conscients des risques auxquels ils peuvent être exposés, et que les activités de mule bancaire peuvent avoir des conséquences importantes pour leur avenir;

E. considérant que les véritables criminels ne seront pas lésés tant que les institutions financières ne seront pas en mesure d'échanger des données;

F. considérant que 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 (règlement général sur la protection des données), exige un motif de traitement valable pour autoriser l'échange de données;

G. considérant que les institutions européennes sont également de plus en plus préoccupées par la fraude sur le web et reconnaissent la lutte contre celle-ci comme un intérêt légitime;

H. vu le système de prévention des risques (*Risk Warning System*) appliqué par les institutions financières des Pays-Bas pour entamer une enquête mutuelle en cas de soupçon de blanchiment d'argent;

DEMANDE AU GOUVERNEMENT FÉDÉRAL:

1. de procéder à un échange de bonnes pratiques avec les Pays-Bas, où les institutions financières utilisent déjà

VOORSTEL VAN RESOLUTIE

DE KAMER VAN VOLKSVERTEGENWOORDIGERS,

A. gelet op de exponentiële groei van cybercriminaliteit in de afgelopen jaren;

B. overwegende dat criminelen vaak gebruik maken van zogenaamde geldezels om het geld dat zij door middel van frauduleuze praktijken afhandig maken van hun slachtoffers door te sluizen naar andere bankrekeningen, om zo onzichtbaar te blijven;

C. aangezien de zogenaamde geldezels risico lopen op een veroordeling, maar ook op een zwarte lijst kunnen terechtkomen bij de bank, waardoor zij in de toekomst mogelijk geen zichtrekening of lening meer krijgen;

D. aangezien vaak jongeren dienst blijken te doen als geldezels, zij zich vaak niet voldoende bewust zijn van de risico's die zij kunnen oplopen en het optreden als geldezel ingrijpende gevolgen kan hebben voor hun toekomst;

E. overwegende dat de echte criminelen buiten schot blijven zolang financiële instellingen niet tot een uitwisseling van gegevens kunnen overgaan;

F. 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 (algemene verordening gegevensbescherming), dat een geldige verwerkingsgrond vereist om de beoogde gegevensuitwisseling toe te staan;

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

H. gelet op het *Risk Warning System*, dat in Nederland gebruikt wordt door de financiële instellingen om een onderling onderzoek te starten bij een vermoeden van het witwassen van geld;

VERZOEK DE FEDERALE REGERING:

1. best practices uit te wisselen met Nederland, waar financiële instellingen reeds een *Risk Warning System*

un système de prévention des risques (*Risk Warning System*) pour lutter contre la fraude et le blanchiment d'argent;

2. d'organiser une concertation structurelle avec le secteur financier, mais aussi avec la police, le parquet et les opérateurs des télécommunications de notre pays afin de cartographier ce problème et de débattre des solutions envisageables;

3. d'élaborer un cadre légal qui permette aux institutions financières d'échanger des informations sur les comptes suspects et les transactions suspectes, en cas de soupçon de blanchiment d'argent, afin de faciliter le démantèlement d'un éventuel réseau criminel;

4. de faire rapport à la Chambre des représentants après un an sur les progrès de la mise en œuvre de la présente résolution.

6 mai 2021

gebruiken om fraude en het witwassen van geld tegen te gaan;

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

3. een wettelijk kader uit te werken om het voor de financiële instellingen mogelijk te maken informatie omtrent verdachte rekeningen en transacties uit te wissen bij een vermoeden van het witwassen van geld, zodat een mogelijk crimineel netwerk makkelijker kan worden opgerold;

4. na één jaar terug te koppelen naar de Kamer van volksvertegenwoordigers over de vooruitgang van de uitvoering van deze resolutie.

6 mei 2021

Michael FREILICH (N-VA)
Joy DONNÉ (N-VA)