IBAN-naamcontrole – wetsvoorstel - advies

1. Inleiding

De commissie voor Economie, Consumentenbescherming en Digitale Agenda heeft Febelfin uitgenodigd om haar een schriftelijk advies te bezorgen over het wetsvoorstel (Michael Freilich c.s.) tot wijziging van het wetboek van economisch recht, teneinde een IBAN-naamcontrole in te voeren om bancaire internet- en cyberfraude tegen te gaan nr. 2296/001.

Febelfin dankt de commissie voor deze gelegenheid om haar standpunt te delen.

Febelfin bestudeert de opportuniteit en haalbaarheid van IBAN-naamcontrole reeds sinds de invoering ervan in Nederland en heeft hierbij een aantal vragen die ertoe hebben geleid dat dit nog niet werd ingevoerd.

Ons advies gaat dieper in op de IBAN-naamcontrole aan de hand van volgende vragen:

- Wat is de Europese context?
- Welke fraudetypes kunnen hiermee worden voorkomen?
- Hoe kan het worden geoptimaliseerd?
- Welke operationele uitdagingen brengt het met zich mee?

Alvorens in te gaan op het wetsvoorstel, lichten we het ruimere kader van de fraudebestrijding toe. We vermelden de vele fraudemitigatiemaatregelen die de sector vandaag reeds toepast of die op korte termijn zullen worden geïmplementeerd. De bestrijding van fraude gebeurt immers niet aan de hand van maatregelen die los staan van elkaar maar vereist een coherent ecosysteem van tegenmaatregelen.

Los van onderstaande elementen begrijpen wij natuurlijk ten volle dat er hoge verwachtingen zijn naar fraudemitigatie onder meer via IBAN-naamcontrole. Hoewel uit onderstaande analyse in eerste instantie zou kunnen blijken dat wij ons terughoudend opstellen tegenover de IBAN-naamcontrole, wensen wij te benadrukken dat Febelfin zich constructief wenst te overleggen over de optimale aanpak.

2. Fraudebestrijding: het ruimere kader

De banken leveren enorm veel inspanningen om frauduleuze betalingen te voorkomen. Banken hebben verschillende systemen ingebouwd om transacties veilig te laten verlopen en de betalingsfraude zo veel mogelijk te voorkomen en/of in te dijken. Zo wordt er sinds een tiental jaar tweestapsauthenticatie toegepast bij online en mobiel bankieren. De klant identificeert zichzelf aan de hand van twee elementen – een kaart of telefoon, een pincode, een vingerafdruk of een gezichtsscan – om e-betalingen te initiëren.

De banken investeren in intensieve monitoring op uitgaande betalingen en maken op die manier veel schade ongedaan. Deze inspanningen leveren opmerkelijke resultaten: meer dan 75% van alle frauduleuze overschrijvingen (waarvoor een gephishte responsecode werd gebruikt) wordt door de banken geblokkeerd of teruggevorderd.
Bovendien overleggen de banken om een doorgedreven, adequate monitoring in te voeren van de inkomende betalingen, in overeenstemming met de marktomstandigheden en de evolutie van de fraudes.

Ook wordt volop ingezet op sensibiliseringsacties, waarbij we iedereen willen oproepen om waakzaam te zijn voor phishing en online fraude. Campagnes met tips, zowel op sociale media als op tv en radio, bereikten een groot doelpubliek. Maar het aantal fraudegevallen blijft toenemen en dus is er nog werk aan de winkel. Sensibiliseringscampagnes zullen altijd belangrijk blijven, maar de financiële sector doet veel meer dan dat.

Cyberfraude is uitgegroeid tot een maatschappelijk probleem. De fraudeurs slaan alsmaar meer toe en door hun diverse manier van werken, blijft geen enkele sector gespaard. Iedereen is betrokken partij en dat maakt van online veiligheid een gedeelde verantwoordelijkheid. Alleen samen kunnen we deze strijd aan. Zo lopen er initiatieven in samenwerking met telecomoperatoren, parket, politie, overheidsinstanties en justitie om cyberfraude in al zijn dimensies en verschijningsvormen aan te pakken.

Febelfin dringt aan op een wettelijke regeling voor een zogenaamd “Risk Warning System” waarmee informatie over betrokkenen bij betalingsincidenten kan worden uitgewisseld onder banken om verdere incidenten door die betrokkenen te voorkomen. Het betreft hier vooral “geldezels” die ontvreemd geld doorsluizen. Een voorstel van resolutie betreffende het bestrijden van cyberfraude via geldezels werd in de Kamer van volksvertegenwoordigers op 17/2/2022 besproken.

Febelfin dringt ook aan op een gepaste organisatie en meer middelen bij de politie en parket om de fraudeurs optimaal op te sporen en te vervolgen.

3. Analyse

Wat is de Europese context?

Er vinden momenteel Europese raadplegingen plaats in het kader van de herziening van de tweede betalingsdienstenrichtlijn[1] en de *Retail Payments Strategy*[2] die o.a. kijkt naar het voorkomen van fraude bij instant betalingen. Europa denkt hierbij niet alleen aan een IBAN-naamcontrole vóór initiatie van de overschrijving (zoals voorgesteld in het wetsvoorstel) maar ook aan IBAN-naamcontrole na uitvoering van de overschrijving. Het is nog niet duidelijk hoe en of de betaaldienstenrichtlijn hiervoor zou worden aangepast. De Europese Commissie heeft aangekondigd dat ze in kader van haar *Retail Payments Strategy* haar voorstel/beslissing zal bekendmaken in het vierde trimester van dit jaar.

Bijgevolg stelt zich de vraag of een nationale wettelijke regulering momenteel aangewezen is. Nationale initiatieven zouden best worden afgestemd met Europa om te voorkomen dat nationale regulering haaks op Europese regulering zou komen te staan.

We herinneren er ook aan dat in Nederland en het Verenigd Koninkrijk de IBAN-naamcontrole niet werd ingevoerd bij wet maar respectievelijk markt gedreven en door de bankentoezichthouder.

Welke fraudetypes kunnen worden voorkomen met IBAN-naamcontrole?

Er zijn vele vormen van internetfraude en oplichters passen hun modi operandi continu aan in functie van de verbetering van tegenmaatregelen.

IBAN-naamcontrole helpt niet ingeval er gemeld wordt “Geen overeenkomst” en hiermee geen rekening wordt gehouden (zodat de overschrijving wordt bevestigd). Dit is onder meer het geval voor de belangrijkste modi operandi:

- Phishingfraude want de oplichter initieert de overschrijvingsopdracht en negeert uiteraard de melding “Geen overeenkomst”;
- Kluisrekeningfraude (bankhelpdeskfraude) want het slachtoffer wordt via “social engineering” gemanipuleerd om de melding “Geen overeenkomst” te negeren of de correcte naam van de geldezel wordt gebruikt.

[1] 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
[2] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0592&from=EN

In Nederland is de IBAN-naamcontrole voorzien maar de Nederlandse Vereniging van Banken (NVB) meldt op 17/11/2021 “De totale schade als gevolg van phishing (6,1 miljoen euro) en bankhelpdeskfraude (16,5 miljoen euro) kwam in de eerste zes maanden van 2021 uit op ruim 22,5 miljoen euro.”.

IBAN-naamcontrole helpt niet ingeval er gemeld wordt “ja/bijna overeenkomst” omdat de oplichter aan het slachtoffer de naam van de geldezel als begunstigde heeft opgegeven en het slachtoffer dit heeft aanvaard. Dit is dikwijls/meestal het geval bij vriendschapsfraude, emofraude, beleggingsfraude en CEO-fraude.

Indien de oplichter een rekeningnummer van begunstigde/geldezel gebruikt in het buitenland dan wordt er gemeld “Bevestiging van een onbeschikbare begunstigde” en helpt de IBAN-naamcontrole niet. Bij de meeste factuurfraude wordt reeds een buitenlands rekeningnummer gebruikt en van zodra IBAN-naamcontrole wordt ingevoerd, zullen oplichters meestal een buitenlands rekeningnummer gebruiken.

Factuurfraude komt meestal voor bij professionelen die echter gebruik maken van betalingssoftware om betalingsbestanden aan te maken en op te sturen naar hun bank. Hierbij is er geen online interactie tussen de opdrachtgever en zijn bank voor elke overschrijving. Bijgevolg is IBAN-naamcontrole hier niet van toepassing tenzij er in de betalingssoftware een speciale verbinding zou worden ingebouwd via een zogenaamde “Application Program Interface” (API).

Bijgevolg zal IBAN-naamcontrole slechts een kleine fractie van de fraude reduceren en aangezien oplichters voor factuurfraude snel zullen uitwijken naar buitenlandse rekeningnummers of andere modi operandi zullen aanwenden, wordt een zeer beperkt fraudereductie verwacht.

Tot slot merken we op dat de (belangrijkste) aanleiding voor IBAN-naamcontrole in Nederland niet relevant is in België. In Nederland werden afgesloten rekeningnummers op korte termijn toegewezen aan nieuwe rekeninghouders. Bijgevolg werden overschrijvingen naar dergelijke rekeningnummers in een lijst van vertrouwde begunstigden naar de verkeerde rekeninghouder gestuurd. Via IBAN-naamcontrole voorkomt met dit in Nederland. Dit probleem stelt zich echter niet in België aangezien afgesloten rekeningnummers niet worden toegewezen aan nieuwe rekeninghouders.

De fraudereductie van 81 % die wordt gemeld in de toelichting bij het wetsvoorstel wordt in vraag gesteld aangezien een andere bank in Nederland eerder een zeer beperkte fraudereductie meldt omwille van de redenen hierboven toegelicht.

Hoe kan IBAN-naamcontrole worden geoptimaliseerd?

Risico gebaseerde controle

Voor de meeste overschrijvingen is er geen of zeer beperkt frauderisico:

- Oplichters frauderen niet voor kleine bedragen omdat na detectie of klacht de betrokken rekening van de begunstigde geldezel wordt geblokkeerd en afgesloten door de bank en de oplichter kosten oploopt om een nieuwe geldezel te rekruteren. Er is bijgevolg onvoldoende netto "winst" voor oplichters voor kleine bedragen.
- Overschrijvingen naar de geregistreerde lijst van vertrouwde begunstigden;
- In geval gebruik wordt gemaakt van "Request to Pay" (RTP)[3], wordt een betalingsverzoek door de begunstigde met zijn/haar naam en IBAN meestal via zijn/haar bank opgestuurd naar de betaler. Indien hierbij door die bank de IBAN-naamcontrole werd uitgevoerd dan is een extra IBAN-naamcontrole vóór de initiatie door de betaler overbodig.
  RTP wordt reeds gebruikt en veralgemening wordt overwogen als alternatief voor kaartbetalingen, zowel in winkels als op afstand (e-commerce).

De betalingsdienstenrichtlijn verwijst in artikel 98 naar technische reguleringsnormen[4] met "passende beveiliging ten behoeve van betalingsdienstgebruikers en betalingsdienstaanbieders, middels de vaststelling van doeltreffende en risico gebaseerde eisen". Hierin wordt vrijstelling voorzien inzake sterke cliëntauthenticatie onder bepaalde voorwaarden, onder meer kleine bedragen.

Het is aangewezen om analoog voor IBAN-naamcontrole uitzonderingen/vrijstellingen te voorzien op basis van risico gebaseerde voorwaarden. Door vrijstelling voor overbodige controles worden de verwerkingskosten en -tijd drastisch gereduceerd.

In Nederland en het Verenigd Koninkrijk werd de IBAN-naamcontrole progressief ingevoerd, startend met de grootste betalingsdienstaanbieders, vervolgens middelgrote betalingsdienstaanbieders en eventueel later ook kleine betalingsdienstaanbieders. Hiermee wordt rekening gehouden met proportionaliteit en risico wat betreft de betalingsdienstaanbieders. Factuurfraude richt zich niet specifiek op een bank maar is willekeuring gedistribueerd over alle betalers zodat het risico bij betalingsdienstaanbieders proportioneel is aan het aantal klanten.

Minimale frictie voor de betaler

De verplichte meldingen door de verzoekende betalingsdienstaanbieder aan de betaler moeten worden beperkt tot wat strikt noodzakelijk is voor het doel, namelijk het voorkomen van fraude. Extra meldingen kunnen verwarring, misverstanden, frictie… meebrengen bij de betaler zodat deze best optioneel blijven in functie van de situatie.

Als voorbeeld verwijzen we naar de huidige meldingen bij initiatie van overschrijvingen. Ontoereikend saldo wordt gemeld maar niet wanneer er voldoende saldo is. Wanneer de validatie van de controlecijfers in de IBAN negatief is dan wordt dit gemeld, maar niet als dit ok/positief is.

[3] https://www.europeanpaymentscouncil.eu/what-we-do/other-schemes/sepa-request-pay-scheme

[4] Gedelegeerde Verordening (EU) 2018/389 van de Commissie van 27 november 2017 tot aanvulling van Richtlijn (EU) 2015/2366 van het Europees Parlement en de Raad wat betreft technische reguleringsnormen voor sterke cliëntauthenticatie en gemeenschappelijke en veilige open communicatiestandaarden

IBAN-naamcontrole moet de betaler informeren (waarschuwen) minstens ingeval er de door de betaler opgegeven naam van de begunstigde niet overeenkomt met een aan de unieke identificator gekoppelde naam van een rekeninghouder.

Vermelding door de verzoekende betalingsdienstaanbieder van overeenkomst, bijna overeenkomst met vermelding van de overeenkomende naam van de rekeninghouder, of dat de gegevens niet beschikbaar zijn, moeten optioneel blijven voor de verzoekende betalingsdienstaanbieder.

Uitbreiding naar grensoverschrijdend toepassingsgebied

Zoals reeds vermeld is afstemming met Europa aangewezen om grensoverschrijdende interoperabiliteit mogelijk te maken.

IBAN-naamcontrole uitbreiden naar betaalrekeningen aangehouden bij een betalingsdienstaanbieder gevestigd in een land waar eveneens een IBAN-naamcontrole wordt toegepast is afhankelijk van onder meer de technische en financiële voorwaarden van die uitbreiding. De betalingsdienstaanbieders in België mogen niet afhankelijk zijn en overgeleverd worden aan niet-haalbare of onredelijke voorwaarden van een betalingsdienstaanbieder of een derde partij in het buitenland.

Conformiteit inzake de algemene verordening gegevensbescherming

Het advies van de Gegevensbeschermingsautoriteit (GBA) inzake conformiteit met de algemene verordening gegevensbescherming (AVG) dient te worden geanalyseerd.

Welke operationele uitdagingen brengt IBAN-naamcontrole met zich mee?

Niet geschikt voor alle bankkanalen (online versus offline kanalen)

De melding door de betalingsaanbieder aan de betaler kunnen uitsluitend plaatsvinden indien de overschrijving online wordt ingevoerd.

Er vinden echter ook vele overschrijvingen offline plaats via papierformulieren of via betalingsbestanden. Betalingsbestanden worden door professionelen aangemaakt aan de hand van betalingssoftware zonder online verbinding bij de invoering of opmaak van de individuele overschrijvingen. Een melding door de betalingsaanbieder aan de betaler bij invoering vereist een speciaal elektronische informatie-uitwisselingssysteem aan de hand van een zogenaamde “Application Program Interface” (API) dat in de betalingssoftware bij de betaler moet worden geïntegreerd.

Persoonsnaamcontrole impliceert onterechte meldingen

Persoonsnaamcontrole in overschrijvingen is bijzonder complex zoals vermeld in de toelichting bij artikel 2: “er is een groot aantal variabelen te overwegen. Mensen gebruiken onder meer een verkorte vorm van hun naam, een roepnaam of de naam van de echtgenoot. Lange en buitenlandse namen zijn vaak moeilijk te spellen. Zelfs gemakkelijke namen kunnen voor mensen moeilijk te spellen zijn omdat er veel variaties van bestaan (bijvoorbeeld Jansen en Janssen of Freilich, Frejlich, Freylich, Froelich en Frohlich of Van Den Berg, Vanden Berg, Vandenberg, Van Den Bergh, Van den Bergh, Vandenbergh, Van Den Berge, Van den Berge, Vandenberge, Van Den Berghe, Van den Berghe, Vanden Berghe of Vandenberghe). Betalingsdienstaanbieders zijn voor de witwaswetgeving verplicht hun cliënten te identificeren. Zij zullen de wettelijke naam registeren, maar zelfs bij gebruik van de wettelijke naam zal een “bijna overeenkomst” nader moeten worden ingevuld (bijvoorbeeld door te bepalen dat 70 % van de opgegeven ASCI-tekens overeenkomen met de geregistreerde naam).”

Bovendien is er extra complexiteit als gevolg van taalvariaties, afkortingen, merknamen, factoring…

Er wordt bijgevolg door betalingsaanbieders in het buitenland, waar de IBAN-naamcontrole reeds van toepassing is, bij een IBAN-naamcontrole soms onterecht gemeld dat er geen overeenkomst is of dat er wel overeenkomst is zodat de betaler soms onterecht een betaling respectievelijk niet of wel bevestigt.

De aansprakelijkheid van onterechte meldingen is niet duidelijk. De betaler kan immers mogelijks financiële schade leiden door een zogenoemde ‘false positive’, denken we bvb. aan nalatigheidsinteresten bij het te laat betalen van een factuur.

Complex project met lange doorlooptijd

De ontwikkeling en operationalisering van IBAN-naamcontrole is een bijzonder complex project met hoge kosten en lange doorlooptijd. In het buitenland heeft dit jaren geduurd. Men voerde er IBAN-naamcontrole bovendien progressief in met een pilootfase en eerst met de grootste betalingsaanbieders waarvoor de risico’s het hoogst zijn.

Er werd een amendement ingediend om “Centraal aanspreekpunt” (CAP) als “databank te gebruiken voor het verkrijgen van gegevens (naam en rekeningnummer) bij het uitvoeren van IBAN-naamcontrole.”… “Dit vergemakkelijkt de praktische uitvoerbaarheid, versnelt de implementatietijd en verhoogt de privacybescherming, onder andere omdat betalingsdienstaanbieders niet elk afzonderlijk de nodige gegevens dienen te delen.”

Het CAP slaat echter het rijksregister- of ondernemingsnummer van personen op en niet de naam behalve indien het rijksregister- of ondernemingsnummer uitzonderlijk niet beschikbaar zou zijn. Bovendien zijn er vragen over de hoge raadplegingskosten, verwerkingscapaciteit, de vereiste antwoordtijd (fractie van seconde) en beschikbaarheid (24/7 meer dan 99,9 %) en privacybescherming

(mededeling van naam aan verzoekende betalingsdienstaanbieder want CAP voert IBAN-naamcontrole niet uit)…

Er dient bijgevolg minstens anderhalf jaar te worden voorzien om de systemen aan te passen.

4. Besluit

Zoals reeds gemeld in de inleiding dient voorgaande niet te worden geïnterpreteerd als een gebrek aan bereidwilligheid vanuit de sector om mee te werken aan een initiatief om overschrijvingsfraude te mitigeren. Integendeel, Febelfin en haar leden stellen zich constructief op om mee te werken aan de invoering van een IBAN-naamcontrole indien dit een gepaste oplossing blijkt te zijn die ook de steun van Europa kent.

Febelfin en haar leden engageren zich er ook toe om de nodige stappen te zetten om een IBAN-naamcontrole op te zetten conform de beleidskeuzes van Europa in dit kader. Hiervoor dient het Europees wetgevingsproces en omzetting in wet niet te zijn afgerond. Wel wensen wij eerst een garantie dat onze keuze en implementatie op korte termijn niet achterhaald wordt door Europa en onze investeringen grotendeels verloren gaan.