

Position Paper Rondetafelgesprek Online Fraude

In de afgelopen 10 jaar hebben banken een grote verschuiving gezien in online criminaliteit. Waar vroeger vooral werd 'gephist' naar inloggegevens zodat criminelen zelf bij iemands rekening konden, zien we nu veel fraudevormen waarbij klanten worden verleid om zelf geld over te maken. Banken werpen barrières op om hun klanten te beschermen, maar als criminelen klanten overhalen om geld over te maken, is het al te laat. Daarom werken banken samen in publiek-private samenwerkingen om met alle partners in de fraudeketen maatregelen te nemen om criminelen eerder tijdens de 'criminele reis' dwars te zitten.

In aanloop naar het rondetafelgesprek online fraude geven we als Nederlandse Vereniging van Banken (NVB) graag het volgende mee:

- Online fraude is een groot maatschappelijk probleem dat sterk toeneemt door de toenemende digitalisering en groei van het internetgebruik;
- Voor dit blijvende probleem is een structurele publiek-private samenwerking nodig. Zorg daarom voor **meerjarige financiering** voor de **Integrale Aanpak Online Fraude (IAOF)**¹;
- Zorg ervoor dat alle partijen in de fraudeketen hun **verantwoordelijkheid** nemen en maatregelen treffen, met name sociale mediaplatforms.
- Maak **gerichte gegevensdeling** tussen publieke en private partijen mogelijk om online fraude tegen te gaan;
- Richt een **nationaal anti-scam centrum** op zodat interventies sneller plaatsvinden.

Criminal journey en maatregelen over de hele keten

Binnen de integrale aanpak online fraude zijn door banken en ketenpartners zogeheten *criminal journeys* opgesteld: deze beschrijven zes fasen die criminelen doorlopen bij fraude, zoals bankhelpdeskfraude.



¹ De **Integrale Aanpak Online Fraude** is een samenwerking tussen publieke partijen zoals JenV, politie, OM, MinEZ en MinFin, en private partners zoals banken, telecombedrijven, Thuiswinkel.org, de Consumentenbond en VNO-NCW/MKB-Nederland.

Banken zijn pas betrokken vanaf fase 4 – en dan is het vaak te laat.² Op dat moment heeft de crimineel al gegevens van het slachtoffer bemachtigd, contact gemaakt en het slachtoffer overtuigd geld over te maken. Andere partijen kunnen eerder in de keten ingrijpen, waardoor veel meer schade kan worden voorkomen. Zo begint 83% van online fraude via **social media, sms, e-mail of telefoon**. Denk aan een valse SMS of app bericht dat een rekening moet worden betaald, een oproep om je bankrekening eventjes 'uit te lenen' (geldezel) of makkelijk geld verdienen met nepadvertenties waarna je in het web van de fraudeur wordt getrokken.

Criminelen kunnen nog veel te makkelijk anoniem opereren. Daarom is het nodig dat:

- aanbieders van online dienstverlening en telecomproviders de identiteit van hun klanten checken;
- online dienstverleners beter controleren of advertenties echt zijn zodat consumenten niet worden misleid;
- voldoende opsporingscapaciteit beschikbaar is om fraudeurs op te pakken en te vervolgen.

De NVB benadrukt het belang dat iedere organisatie zijn eigen rol en verantwoordelijkheid binnen de fraudeketen kent en neemt.

Integrale aanpak online fraude (IAOF)

De NVB is groot voorstander van de IAOF. Deze samenwerking begint duidelijk vruchten af te werpen: voor diverse fraudevormen zijn criminal journeys en maatregelen opgesteld, en er zijn sterke netwerken van ketenpartners gevormd, waarin vroegtijdig informatie over nieuwe trends en modus operandi wordt gedeeld en gezamenlijk maatregelen worden getroffen. Zo verkent de AFM samen met banken hoe websites van boilerrooms³ sneller op de waarschuwingslijst geplaatst kunnen worden en offline gehaald kunnen worden. Om deze aanpak duurzaam voort te zetten en in te bedden in de maatschappij, is blijvende ondersteuning vanuit de overheid nodig. Wij pleiten daarom voor **meerjarige financiering** van de integrale aanpak via de begroting van Justitie & Veiligheid.

'Line Busy' is een veelbelovende succesvolle interventie binnen de IAOF van banken en telecom om bankhelpdeskfraude te voorkomen. Uit onderzoek van banken blijkt dat slachtoffers in meer dan 75 procent van de gevallen tijdens de frauduleuze overboeking telefonisch in gesprek zijn met de oplichter. Banken willen daarom bij telecomeaanbieders kunnen checken of iemand telefonisch in gesprek is tijdens het overboeken van geld. De gewenste maatregel kan nu niet worden genomen vanwege de onmogelijkheid om gericht gegevens uit te wisselen tussen banken en de telecomsector. Samen met telecombedrijven heeft de NVB zich ingezet voor een wetswijziging, die nu wordt voorbereid door het Ministerie van Economische Zaken, mede dankzij steun vanuit de Tweede Kamer.

Stip op de horizon: een nationaal anti-scam centrum

Wij pleiten ook voor een nader op te richten nationaal anti-fraudecentrum waar publieke en private partijen informatie delen en samenwerken, binnen een **'fraude-hub'**. Door informatie over frauduleuze activiteiten vroegtijdig te delen, kunnen interventies sneller plaatsvinden en meer fraude worden voorkomen.

Een dergelijke vorm van samenwerking is effectief gebleken. Internationale voorbeelden laten zien dat fysieke samenwerking en directe interventiemogelijkheden – zoals het blokkeren van bankrekeningen, social media accounts, telefoonnummers en IP-adressen – cruciaal zijn voor een slagvaardige aanpak.⁴ Effectieve samenwerking vereist echter goede mogelijkheden voor gegevensdeling. Die zijn momenteel beperkt. Wij roepen de overheid op om gericht gegevens delen mogelijk te maken.

² De inzet van banken leidt aantoonbaar tot een daling van de schade, onder meer door effectieve technische maatregelen zoals het verlagen van daglimieten, het instellen van tijdsloten bij limietverhogingen, het toepassen van spaarsloten op spaarrekeningen en bewustwordingsinitiatieven zoals 'Check het gesprek'.

³ Een boiler room is een verzamelnaam voor personen en organisaties die met behulp van gehaate verkopers mogelijke beleggers benaderen om ze over te halen te investeren in waardeloze of nepbeleggingen.

⁴ Denk aan het Singapore Anti-Scam Command, het Australian National Anti-Scam Centre en het Canadian Anti-Fraud Centre.