

POSITION PAPER

Fraudepreventie (CIFAS)

Digitale criminaliteit is een toenemend maatschappelijk probleem dat veel impact heeft op Nederlandse burgers. De bankensector heeft zichzelf de ambitie gesteld om Nederland het minst aantrekkelijke land voor digitale criminaliteit te maken. Hiermee beschermen we burgers tegen fraude. Banken hebben eerder gepleit voor een integrale cross-sectorale aanpak met regie van de overheid, waarbij digitale communicatiekanalen (computers, tablets, smartphones) beter worden beveiligd om oplichting te voorkomen, mensen digitaal weerbaarder worden gemaakt en gegevensdeling wordt ingezet om fraude te voorkomen, te bestrijden en de pakkans te verhogen. Banken begrijpen de behoefte van het MKB om meer aan preventie van fraude te doen. Een fraudepreventiesysteem zoals CIFAS zou kunnen bijdragen aan het voorkomen van fraude.

Een groot maatschappelijk probleem

Online werken, het onderhouden van sociale contacten en het doen van betalingen is in een stroomversnelling geraakt. Deze digitalisering leidt tegelijkertijd tot een stijging van digitale fraude. Dit is een breed maatschappelijk probleem. Bij klanten van banken, maar ook in andere bedrijfssectoren is waarneembaar dat criminelen misbruik maken van digitale dienstverlening en zich snel nieuwe methodes eigen maken. In het eerste halfjaar van 2021 bedroeg de schade van phishing en bankhelpdeskfraude al 22,5 miljoen euro¹. Achter deze cijfers gaan vele persoonlijke drama's schuil.

De rol van gegevensuitwisseling bij de bestrijding van fraude

Door middel van het uitwisselen van gegevens kan fraude effectief bestreden worden. Gegevensuitwisseling levert daarnaast veel kennis en inzichten op over digitale criminaliteit die noodzakelijk zijn om criminaliteit te bestrijden. Gegevensuitwisseling is daarom nodig om te voorkomen dat Nederland steeds aantrekkelijker wordt voor criminaliteit. Dergelijke informatiedeling brengt ook risico's met zich mee. Het is van belang dat deze informatiedeling zorgvuldig en verantwoord wordt uitgevoerd. Met minimale gegevensuitwisseling zoals bijvoorbeeld het uitwisselen en matchen van IP adressen of IMEI nummers zou al betere fraudepreventie kunnen worden gedaan dan nu. De bankensector pleit daarom voor beheerste en doelmatige cross-sectorale gegevensuitwisseling onder regie van de overheid in de bestrijding en het voorkomen van fraude.

¹ [Stijging schade als gevolg van digitale fraude maakt gezamenlijke aanpak noodzakelijk \(nvb.nl\)](#)

Steeds meer mogelijkheden om fraude te voorkomen

Voor particulieren ontstaan steeds meer mogelijkheden om voorafgaand aan een transactie een aantal checks op legitimiteit te doen, bijvoorbeeld een controle op de website², het IBAN (banknummer), e-mailadres, telefoonnummer en de betaallink³. Daarnaast hebben de banken met de introductie van de IBAN-naamcheck hun klanten ook een belangrijk instrument gegeven waarmee zij, voordat de betaling wordt uitgevoerd, informatie krijgen over de combinatie van naam en bijbehorend rekeningnummer. Deze initiatieven en andere initiatieven spelen een belangrijke rol in het voorkomen van fraude en het beschermen van burgers. Ook commerciële aanbieders richten zich op systemen die je kunt gebruiken ter voorkomen van fraude⁴.

Hoe wisselen banken op dit moment gegevens uit?

Banken hebben zelf inmiddels veel ervaring opgedaan met gegevensuitwisseling. In het Protocol Incidentenwaarschuwingssysteem Financiële Instellingen (PIFI) staat wanneer en onder welke voorwaarden gegevens van (rechts)personen die een risico vormen voor een bank of de sector kunnen worden uitgewisseld. Deze gegevens kunnen tussen banken onderling worden uitgewisseld ten behoeve van onderzoek naar incidenten. Onder strikte voorwaarden kunnen verwijzingsgegevens van een (rechts)persoon in het Extern Verwijzingsregister (EVR) worden geregistreerd. Financiële instellingen die ook zijn aangesloten bij het PIFI kunnen deze gegevens via het EVR raadplegen zodat bij de aanvraag van een product of dienst bij de verstrekking daarvan een gewogen besluit kan worden gemaakt. Het PIFI voldoet aan de Algemene Verordening Gegevensverwerking (AVG). Voor deze uitwisseling is een vergunning verstrekt door de Autoriteit Persoonsgegevens⁵. In deze vergunning staan de criteria waaronder de uitwisseling van gegevens plaats kan vinden en ook de waarborgen bij deze gegevensverwerking. Ook de rechten van de (rechts)persoon, die in lijn zijn met de AVG, staan hierin vermeld.

Hoe kan cross-sectorale gegevensuitwisseling burgers beschermen?

Ook (klanten van) andere sectoren worden getroffen door de ernstige gevolgen van digitale fraudes. Het delen van gegevens met andere sectoren stelt het Nederlandse bedrijfsleven in staat om burgers en de maatschappij effectiever te beschermen tegen fraude. Gegevensuitwisseling kan meerdere vormen aannemen. Zo kunnen bijvoorbeeld IP (internet) adressen of IMEI (mobiele telefoon) nummers gedeeld worden met onder andere handelsplatformen, sociale media, telecompartijen en internetproviders om mogelijke vormen van fraude te voorkomen. De gegevensdeling heeft dus vooral een sterke preventieve werking. Bekende daders kunnen zo moeilijker opnieuw toeslaan.

² [Controleer verkopergegevens | politie.nl](https://www.politie.nl)

³ [Checkjelinkje - checkjelinkje.nl](https://www.checkjelinkje.nl)

⁴ [Scam Adviser | scamadviser.com](https://www.scamadviser.com)

⁵ [Incidenten- waarschuwingssysteem financiële instellingen | Autoriteit Persoonsgegevens](https://autoriteitpersoonsgegevens.nl)

Gegevensuitwisseling op basis van stevige waarborgen

De bankensector neemt veel zichtbare en onzichtbare maatregelen om burgers te beschermen tegen digitale criminaliteit. In aanvulling daarop is cross-sectorale gegevensdeling tussen banken en andere sectoren noodzakelijk om het maatschappelijke probleem van fraude nog effectiever te voorkomen en te bestrijden.

Op dit moment is nog veel onduidelijkheid over de uitwerking van het voorgestelde cross-sectorale fraudepreventiesysteem. Hoe dan ook zal dit gepaard moeten gaan met stevige waarborgen. De gegevensuitwisseling zal altijd moeten plaatsvinden o.b.v. duidelijk afgebakende definities en doelstellingen, met een duidelijke juridische basis en stevige privacy waarborgen rondom bijvoorbeeld proportionaliteit, subsidiariteit, bewijs- en registratievoorwaarden en registratietermijnen.

Banken vinden het van belang dat de overheid een regierol krijgt bij deze aanpak en de kaders schetst voor cross-sectorale gegevensuitwisseling. De overheid kan tevens erop toezien dat de juiste waarborgen worden geïmplementeerd om te voorkomen dat het systeem leidt tot ongewenste uitsluiting van diensten.

Conclusie

De banken vinden het voorgestelde systeem een verkenning waard en zullen de ontwikkelingen op dit gebied nauwlettend volgen. Via de NVB nemen zij graag deel aan de dialoog hierover.

Nederlandse Vereniging van Banken

De Nederlandse Vereniging van Banken behartigt de gemeenschappelijke belangen van de bankensector. Banken zijn van belang voor iedereen. We zijn de verbindende schakel tussen de bankensector, politiek en stakeholders. Samen met deze partijen werken we proactief aan: een dienstbare, stabiele en competitieve bankensector.