

Bank van de Toekomst

Wanneer klanten onderdeel worden van de aanval: alles over cognitieve manipulatie op grote schaal

Oplichting, geldezels en de volgende fase van financiële criminaliteit in Nederland



Fraude buiten de bank om?

De gevaarlijkste aanname in de financiële criminaliteit van vandaag is dat het risico op fraude buiten de bank ligt. Maar in Europa, en dus ook in Nederland, gaat die aanname niet langer op.

De belangrijkste verandering is niet dat klanten frauduleuze betalingen initiëren, dat is al veel langer het geval, maar dat het gedrag van de klant zelf de belangrijkste aanvalsvector is geworden. Gewone rekeninghouders worden heden ten dage geïnstrueerd, gedwongen of gemanipuleerd om betalingen te initiëren, geld te ontvangen, rekeningen te openen en geld over te maken namens criminele netwerken. In veel gevallen geloven ze zelfs dat ze daarbij legitiem, verantwoordelijk of behulpzaam handelen; hen ervan overtuigen dat het tegendeel waar is, kan behoorlijk moeilijk zijn.

Toename geldezels

Deze verschuiving heeft ingrijpende gevolgen voor de digitale economie van onze regio. In heel Europa, en met name in Nederland vanwege de hoge adoptie van digitaal bankieren, weerspiegelen de risico's die verbonden zijn aan realtime betalingssystemen steeds meer de wereldwijde ontwikkelingen. De snelle invoering van SEPA Instant Payments (waarbij betalingen binnen circa 10 seconden worden afgewikkeld) heeft de beschikbare tijd voor fraudedetectie, interventie en terugvordering van geld aanzienlijk verkort. De European Payments Council (EPC) waarschuwt dat instant betaalinfastructuren waarschijnlijk zullen leiden tot een toename van het gebruik van 'geldezels' en stromannen en een versnelling van fraudeschema's, omdat geld vrijwel direct kan worden doorgesluisd. In 2024 meldden de Europese Bankautoriteit (EBA) en de Europese Centrale Bank (ECB) dat fraude met creditcardtransfers in Europa verantwoordelijk was voor ongeveer € 2,2 miljard aan verliezen, waarbij consumenten het grootste deel van de financiële schade leden.¹

Daarbij is het goed om te benadrukken dat veel oplichtingspraktijken niet eens worden gemeld. Andere worden opzettelijk opgesplitst via netwerken van tussenpersonen die transacties verdelen in kleinere stromen, de detectie vertragen en waarde naar het buitenland sluizen voordat terugvordering mogelijk is. Waar het anno 2026 om gaat, is niet of de officiële cijfers over de verliezen jaarlijks stijgen of dalen, maar of de capaciteit, snelheid en slimmigheid van de oplichtingsinfrastructuren zullen blijven toenemen.



500 mln – 1 bln dollar per jaar.

Wereldwijd worden de geschatte verliezen door oplichting gemeten in de honderden miljarden, waarbij sommige analyses het bedrag schatten tussen de 500 miljard en 1 biljoen dollar per jaar. Dit benadrukt dat wat Nederland meemaakt geen uitzondering is, maar onderdeel van een systemische verschuiving.

1: 2024 Payments Threats and Fraud Trends Report, European Banking Authority & European Central Bank (Report on Payment Fraud 2024), DNB/De Nederlandsche Bank, Betaalvereniging Nederland.

Wat er nodig is:

een verschuiving van het opsporen van fraude door derden naar systemen die anticiperen op menselijke manipulatie in het besluitvormingsproces – en organisaties voorbereiden op het risicolandschap van de toekomst.

De trend is duidelijk: frauduleuze praktijken worden steeds professioneler, veerkrachtiger en meer adaptief. Ze zijn erop gericht om gevestigde fraudesystemen te omzeilen en inmiddels óók om de menselijke factor tussen digitale controles en onomkeerbare betalingen uit te buiten.

Bij deze geraffineerde aanpak wordt de klant niet misleid om toegang te verlenen. Hij wordt overgehaald om te handelen. En zodra een betaling door de klant is geautoriseerd, zijn zelfs de sterkste controles van de bank niet langer toegerust om in te grijpen.

De risico's hiervan zijn operationeel, verhogen het risico op reputatieschade en zijn in toenemende mate ook regelgevend. Wat nu nodig is, is een verschuiving van het opsporen van fraude door derden naar het ontwerpen van systemen die anticiperen op menselijke fouten in het besluitvormingsproces – en het voorbereiden van organisaties op het risicolandschap van de toekomst.

Van los incident naar totale infrastructuur

Moderne oplichtingspraktijken gedragen zich minder als gelegenhedscriminelen en meer als gedistribueerde systemen. Hun succes hangt af van orkestratie, timing en schaal, in plaats van een enkel punt van zwakte. Het zijn geen losse, spontane gebeurtenissen of geïsoleerde daders. De scammers van nu zijn georganiseerde, modulaire operaties, ontworpen om te schalen, zich aan te passen en te blijven bestaan, alsof het legitieme bedrijven in een scale-up fase zijn. Elke laag van de operatie – van het eerste phishingberichtje tot het netwerk van geldezels dat gestolen geld verplaatst – is onafhankelijk bemand en geoptimaliseerd, waardoor het hele systeem opmerkelijk bestand is tegen verstoringen van buitenaf. Als één onderdeel wordt uitgeschakeld, blijft de rest van het netwerk gewoon functioneren. Bestaande controle- en handhavingsmethoden, gebaseerd op individuele verdachten en afzonderlijke criminele handelingen, zijn niet ontworpen om dergelijke systemen te bestrijden.

Deze structurele evolutie van fraude wordt steeds zichtbaarder. Europol heeft herhaaldelijk gewaarschuwd dat online fraudenetwerken in Europa nu inderdaad functioneren als sterk georganiseerde criminele ecosystemen met gespecialiseerde rollen, waaronder recruiters, social-engineering-operators, managers van geldezelnetwerken, specialisten in cryptowitwassen en facilitators die frauduleuze bankrekeningen en lege vennootschappen aanbieden. Europese criminele groepen beschouwen bankrekeningen, betaalkaarten, digitale portemonnees en bedrijfsentiteiten steeds vaker als 'wegwerpinfrastructuur' die snel kan worden vervangen wanneer de opsporingsdruk toeneemt.²

De Internet Organised Crime Threat Assessment (IOCTA) en Serious and Organised Crime Threat Assessment (SOCTA) van Europol beschrijven fraudeoperaties als schaalbare, op diensten gebaseerde modellen waarin verschillende criminele actoren modulaire mogelijkheden "als een dienst" aanbieden, waaronder de werving van geldezels en het witwassen van transacties.

2: 2024 Payments Threats and Fraud Trends Report, European Banking Authority & European Central Bank (Report on Payment Fraud 2024), DNB/De Nederlandsche Bank, Betaalvereniging Nederland.

Social engineering

Zoals gezegd opereren criminele groeperingen met een discipline die vergelijkbaar is met die van legitieme organisaties. Ze ontwerpen wervingscampagnes om beïnvloedbare personen te identificeren. Ze verfijnen scripts door middel van testen. Ze beheren zogenaamde 'mule accounts' als voorraad, inclusief onboarding, monitoring, roulatie en verwijdering naar behoefte. Geld wordt via gelaagde kanalen geleid om tracering en terugvordering te voorkomen.

Het is cruciaal om te weten dat deze set-ups ontworpen zijn om te interageren met bankcontroles. In plaats van blindelings detectie te ontwijken, passen ze zich in realtime aan:



Wanneer
waarschuwingen
verschijnen, verandert
het script.



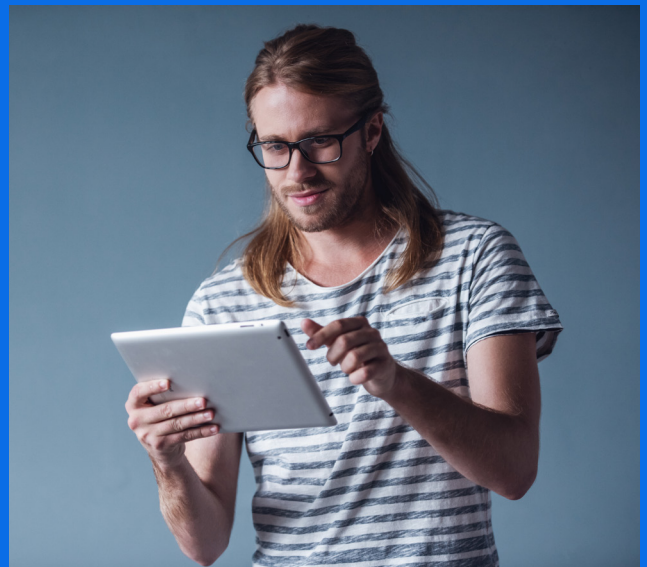
Wanneer limieten van
toepassing zijn, passen
transactiepatronen
zich aan.



Wanneer één kanaal
wordt aangescherpt,
wordt een ander
geopend.

Net als de meeste grote organisaties implementeren ze AI-tools om te testen welke aanpak succesvol is bij welke instellingen en om te schalen wat werkt.

Deze oplichtingspraktijken worden al lang van tevoren bedacht, nog voordat er geld wordt overgemaakt. Social engineering, een belangrijk onderdeel ervan, speelt zich af via telefoongesprekken, berichten en platforms buiten het bereik van de bank, waarbij financiële transacties fungeren als een uitvoeringsstap in plaats van het startpunt.





“Nederlandse banken hebben fors geïnvesteerd in fraudebestrijding en veel van die systemen doen precies waarvoor ze ontworpen zijn. Het probleem is dat oplichting niet langer op transactieniveau verkeerd gaat. Oplichting begint al eerder, waarbij oplichters klanten al vroeg in hun val lokken en het valse verhaal inbedden door middel van verschillende fasen van ‘vertrouwen’ opbouwen. Tegen de tijd dat een traditioneel fraudealarm afgaat, is de mogelijkheid om schade te voorkomen vaak al verkeken.”

SARAH CASSIDY

Fraude-expert, FICO

Dit verklaart waarom volwassen en goedbedoelende fraudebestrijdingsteams in de banksector terecht kunnen stellen dat hun systemen werken, zelfs terwijl het aantal gevallen van oplichting blijft toenemen. De systemen functioneren zoals bedoeld, maar ze zijn ontworpen om identiteitsfraude en ongeoorloofd gebruik te voorkomen. Ze zijn niet ontworpen om cognitieve manipulatie op grote schaal te beheeren.

Scam tijdlijn



Verantwoordelijkheid zonder controle

Er is een verschuiving merkbaar in Europa, waarbij toezichthouders, banken en betalingsautoriteiten zich steeds meer richten op **proactieve interventie en consumentenbescherming** in plaats van zich uitsluitend te richten op fraudedetectie. De meeste Europese landen combineren een hoge digitale adoptie met een snelgroeiende infrastructuur voor directe betalingen, wat leidt tot een toenemende spanning tussen frictieloze betalingen en de verantwoordelijkheid voor fraudepreventie.

Toezichthouders, waaronder de Europese Bankautoriteit (EBA), de Europese Centrale Bank (ECB) en De Nederlandsche Bank (DNB), benadrukken steeds vaker dat instellingen de gedragsindicatoren van manipulatie, social engineering en geldezelactiviteiten eerder in de betalingsketen moeten identificeren, met name in gevallen van fraude met geautoriseerde pushbetalingen (APP). De invoering van verplichte regels voor “Verificatie van begunstigde” (verification of payee) onder de EU-verordening inzake directe betalingen weerspiegelt deze verschuiving van basale transactiemonitoring naar preventieve interventie vóórdat geld wordt overgemaakt. Europol en verschillende Europese bankorganisaties hebben ook hun bezorgdheid geuit over de werving van geldezels, wegwerprekeningen en snelle witwaspraktijken via directe betalingen en cryptovaluta, vooral wanneer legitiem klantgedrag wordt gemanipuleerd in plaats van dat systemen direct worden gecompromitteerd.



Van Nederlandse banken wordt verwacht dat ze schade moeten voorkomen die voortvloeit uit betalingen die worden genomen onder misleiding of dwang.

Nederland wordt vaak gezien als behoorlijk geavanceerd op dit gebied, vooral dankzij het IBAN-systeem, de sterke interbancaire samenwerking en de nauwe coördinatie tussen banken, politie, justitie en fraudebestrijdingsorganisaties. Nederlandse banken staan echter voor dezelfde structurele uitdaging die wereldwijd steeds vaker voorkomt: van hen wordt verwacht dat ze schade moeten voorkomen die voortvloeit uit betalingen die klanten technisch gezien zelf autoriseren, óók wanneer die beslissingen worden genomen onder misleiding, dwang of psychologische manipulatie. Dit heeft de verwachtingen ten aanzien van klantmonitoring, transacties, waarschuwingsmechanismen, gedragsanalyse en interventiebevoegdheden aanzienlijk verhoogd. In de praktijk evolueert de verantwoordingsnorm in Nederland geleidelijk van “is de fraude ontdekt?” naar “had de voorzienbare schade redelijkerwijs kunnen worden voorkomen?”. Dit creëert een structurele spanning: één die banken niet alleen met controles kunnen oplossen.

Grootschalige dwang: ook een 'AI-tool'

De grootste verschuiving in oplichting in de afgelopen twee jaar is hoe psychologische dwang nu via technologie wordt opgeschaald. Generatie AI heeft identiteitsfraude en bedrog enorm versneld, waardoor dreigingen met arrestatie of inbeslagname van rekeningen, valse baan- en beleggingsaanbiedingen en zelfs langdurige romantische manipulatie overtuigender en winstgevender zijn geworden.

Europese toezichthouders waarschuwen dat moderne fraude nu minder wordt gedreven door technische inbreuk, maar meer door psychologische manipulatie op grote schaal. Europol heeft herhaaldelijk social engineering, identiteitsfraude, deepfake-fraude en AI-ondersteunde fraude aangemerkt als snelgroeiende bedreigingen, waarbij slachtoffers vrijwillig overboekingen initiëren onder druk, angst, urgentie of vals vertrouwen.

Ook de Nederlandsche Bank, de NVB en de politie wijzen op de toename van fraude via de helpdesk van banken, valse beleggingsplatformen, romantische oplichting, WhatsApp-identificatie en spoofing-aanvallen waarbij klanten zelf transacties uitvoeren nadat ze zijn gemanipuleerd om te geloven dat ze hun geld beschermen of verantwoordelijk handelen.

Dat sterke authenticatie en technische controles alleen onvoldoende zijn wanneer de klant psychologisch wordt gedwongen de betaling te autoriseren, wordt ook steeds meer erkend door Europese instellingen. De combinatie van generatieve AI, stemklonen, vervalste communicatie en zeer gerichte social engineering-campagnes heeft oplichtingspraktijken overtuigender, schaalbaarder en moeilijker te detecteren gemaakt met traditionele fraudebestrijdingsmethoden.

Als reactie hierop verschuift Europa geleidelijk naar een breder interventiemodel dat gedragsanalyses, realtime waarschuwingen, uitgestelde betalingsuitvoering in risicovolle gevallen, verificatie van rekeningnamen, een krachtigere aanpak van geldezel-accounts en een grotere institutionele verantwoordelijkheid voor voorzienbare schade omvat. Toezichthouders evalueren steeds vaker niet alleen of de fraudebestrijdingsmethoden technisch functioneerden, maar ook of instellingen gedragsindicatoren van manipulatie vroegtijdig herkenden om effectief in te grijpen.

Vanuit strategisch oogpunt is de belangrijkste implicatie voor Nederlandse financiële instellingen dat fraudepreventie niet langer alleen als een probleem op het gebied van cybersecurity, transactiefraude of AML kan worden beschouwd. Het vereist steeds vaker een gecombineerde aanpak die gedragsrisico's, consumentenbescherming en operationele flexibiliteit omvat. Instellingen die de komende jaren naar verwachting het beste zullen presteren, zijn die instellingen die realtime betalingsmonitoring, cross-channel klantrisico-informatie, AI-ondersteunde anomaliedetectie en menselijke interventiemogelijkheden integreren die specifiek zijn ontworpen voor fraudescenario's met dwang. Dit betekent ook een nauwere coördinatie tussen banken, telecomproviders, sociale-mediaplatformen, betaalproviders en wetshandhavers, omdat het aanvalsveld zich nu veel verder uitstrekt dan alleen binnen het banksysteem.





2,4 mln

burgers getroffen door
online criminaliteit



9,4%

9,4% van de bevolking
ondervond online fraude,
was 7,6% in 2022



€ 69 mln

gerapporteerde verliezen
in 2025

De toenemende omvang en professionalisering van fraude in Nederland is zichtbaar in de cijfers. Volgens het CBS werden in 2024 ongeveer 2,4 miljoen Nederlandse burgers getroffen door een vorm van online criminaliteit, waarbij 9,4% van de bevolking online oplichting of fraude ondervond: een aanzienlijke stijging ten opzichte van 2022 (7,6%). De Fraudehelpdesk registreerde in 2024 meer dan 63.000 fraudegevallen, met gerapporteerde verliezen van bijna € 53 miljoen, een stijging van 20% op jaarbasis. Volgens het Nederlandse politierapport Online fraude in beeld 2024 bedroegen de totale geregistreerde online fraudeverliezen in 2023 ongeveer € 109 miljoen, waarvan circa € 33,7 miljoen specifiek gerelateerd aan fraude via de bankhelpdesk en circa € 31 miljoen aan beleggingsfraude. Voor 2025 meldde de Fraudehelpdesk een explosie van gevallen. Het aantal gevallen steeg naar 100.000, een toename van 63% ten opzichte van 2024. De totale gerapporteerde verliezen bedroegen bijna € 69 miljoen. Het aantal getroffen consumenten is ook met 65% gestegen.³

Het is belangrijk om te benadrukken dat zowel Nederlandse banken als politie en justitie stellen dat veel slachtoffers de frauduleuze betalingen persoonlijk goedkeuren nadat ze psychologisch gemanipuleerd of onder druk gezet zijn. ING Bank zag dat fraude via de helpdesk zo wijdverbreid was geworden dat ze speciale realtime verificatiefuncties in haar bankapp introduceerde, waarna het aantal incidenten naar verluidt met 43% daalde.⁴ Onderzoek van de Nederlandse politie wijst er verder op dat deze oplichtingspraktijken ook in Nederland niet langer geïsoleerd en opportunistisch zijn, maar steeds professioneler wordende criminele netwerken die gebruikmaken van grootschalige gestolen datasets, spoofingtechnieken, social engineering en geldezelstructuren om op grote schaal te opereren.⁴

3: Fraudehelpdesk. Persbericht: Druk van oplichters op samenleving was nog nooit zo groot. Fraudehelpdesk, Feb. 2026, www.fraudehelpdesk.nl/wp-content/uploads/2026/02/Persbericht-jaarcijfers-2025-final.pdf.

4: Bekkers, Luuk, Rutger Leukfeldt, and Edward Kleemans. "Police Investigations Into Financial-Economic Cybercriminal Networks: The Experiences and Perceptions of Dutch Law Enforcement." *European Journal on Criminal Policy and Research*, vol. 32, 2026, pp. 305-324. Springer Nature, published 20 Mar. 2025, <https://doi.org/10.1007/s10610-025-09615-2>.

Daarnaast komen er in Nederland ook cryptofraudes voor die meer gebaseerd zijn op overreding dan op technische manipulatie. In verschillende spraakmakende gevallen promootten ‘finfluencers’, zoals [Mo Bicep](#), op sociale media, frauduleuze online cryptohandelpplatformen en moedigden ze volgers aan om te investeren via wat legitieme financiële diensten leken te zijn.

Slachtoffers maakten gewillig geld over in de overtuiging dat ze deelnamen aan winstgevende investeringen, om er vervolgens achter te komen dat de platforms en rendementen verzonnen waren. Wat deze zaken bijzonder moeilijk maakt: het is geen onwetendheid, maar overtuiging. Slachtoffers weten vaak wel dat oplichting bestaat. Ze geloven alleen dat deze interactie die ze nu ervaren legitiem is.

Voor banken zijn de implicaties duidelijk. De eerste signalen van betrokkenheid bij oplichting verschijnen zelden als duidelijke afwijkingen in transacties. Ze komen aan het licht als gedragsverandering: aarzeling, herhaaldelijk negeren van waarschuwingen, ongebruikelijke interacties met apparaten, tegenstrijdige verklaringen of een toenemende urgentie in de loop van de tijd.

Dwang op een dergelijk grote schaal is geen toeval. Het wordt mogelijk gemaakt door complete infrastructuur en operationele omgevingen die ver buiten het bereik van onze huidige (nationale) regelgeving vallen. Om de toekomst van fraude te begrijpen, moeten we daarom verder kijken dan individuele slachtoffers en bankcontroles, naar de wereldwijde economieën die nu gebouwd zijn rond fraudepraktijken.



Merkt op dat de uitdaging minder technisch en meer institutioneel is:

“In Nederland werken banken al met sommige van de meest geavanceerde fraudebestrijdingssystemen ter wereld. Maar oplichters slagen er steeds vaker in om klanten te manipuleren in plaats van systemen te omzeilen. De lastige vraag hier is: wanneer moet je ingrijpen? Veel oplichtingstrajecten lijken op het eerste gezicht nog legitiem, dus instellingen moeten beslissen of ze wachten of handelen wanneer gedragssignalen erop wijzen dat een klant mogelijk al gemanipuleerd wordt.”

RICHARD LAGERWEIJ
Product Manager, FICO

Vroege signalen

Kantelpunten in gedrag

Banken moeten letten op deze subtiele indicatoren:

- 01 Aarzeling tijdens transacties
- 02 Herhaaldelijk negeren van waarschuwingen
- 03 Ongebruikelijke interacties met devices
- 04 Inconsistente verklaringen
- 05 Toenemende urgentie in de loop van de tijd



Hoe de komende vijf jaar eruitzien



De komende 12 maanden

Interventie wordt de maatstaf voor competentie

Dit wordt een cruciaal jaar. Het draait minder om hoe snel instellingen van verdenking naar actie gaan, en meer om hoe vroeg ze bereid zijn in te grijpen.



De komende 36 maanden

Geïndustrialiseerde misleiding

Over een periode van drie jaar zullen oplichtingspraktijken zich verder professionaliseren en opschalen.



De komende 60 maanden

Vertrouwen wordt heropgebouwd of uitgehold

De belangrijkste vraag is niet hoe oplichting eruitziet, maar hoe het vertrouwen in de digitale financiële wereld zich ontwikkelt.



De komende 12 maanden: interventie = competentie?

Dit wordt een cruciaal jaar voor fraude- en oplichtingsbestrijders in Nederland, gezien de toename van fraude en het toegenomen toezicht door toezichthouders. Deze periode zal minder worden bepaald door hoe snel financiële instellingen van verdenking naar actie kunnen overgaan, maar meer draaien om de vraag hoe vroeg ze bereid zijn om in te grijpen.

Realtime betalingen en de bijna directe administratieve afwikkeling laten weinig ruimte voor beraad. Voor “even over nadenken”. In deze situatie is het aloude comfort van wachten op een bevestiging steeds minder verenigbaar met het beperken van schade, de verwachtingen van een toezichthouder en het vertrouwen van de klant. De centrale vraag die banken moeten beantwoorden is: wat is voldoende bewijs om in te grijpen?

Europese toezichthouders, rechtbanken, ombudsdiensten en toezichthoudende instanties gaan geleidelijk aan voorbij het traditionele onderscheid tussen geautoriseerde en ongeautoriseerde betalingen en onderzoeken steeds vaker of financiële instellingen adequaat hebben gereageerd op zichtbare signalen van manipulatie, dwang of afwijkend klantgedrag voordat een frauduleuze betaling werd uitgevoerd.

Binnen de Europese Unie wordt deze ontwikkeling deels gedreven door de groeiende bezorgdheid over fraude met geautoriseerde pushbetalingen (APP), waarbij slachtoffers technisch gezien instemmen met transacties, maar dit doen onder misleiding of psychologische druk. De invoering van verplichte ‘Verificatie van begunstigde’-vereisten in de EU-verordening inzake directe betalingen laat zien dat instellingen proactief voorzienbare schade moeten voorkomen in plaats van uitsluitend te vertrouwen op fraudedetectie achteraf.



Operationele gevolgen

In Nederland richten geschilonderzoek en toezichtbesprekingen zich met name steeds vaker op de vraag of banken voldoende waarschuwingen, escalatiemechanismen en klantbescherming hebben geboden in gevallen van spoofing, fraude via de helpdesk en beleggingsfraude.

Nederlandse rechtbanken en klachteninstanties hebben zich al gebogen over zaken waarin klanten fraudewaarschuwingen negeerden of werden gemanipuleerd om beveiligingsmaatregelen te omzeilen. Daarbij werd ook gekeken of banken redelijkerwijs eerder hadden kunnen ingrijpen op basis van ongebruikelijke gedragspatronen of de transactiecontext. Dit leidt tot een groeiende juridische en operationele spanning: instellingen worden niet alleen beoordeeld op technische naleving of de correcte werking van Strong Customer Authentication, maar ook op de vraag of waarschuwingssignalen van dwang, urgentie, verwarring of manipulatie voldoende werden herkend en of hierop adequaat werd gereageerd tijdens het klanttraject.

Strategisch gezien zal dit waarschijnlijk nog belangrijker worden onder het aankomende PSD3-raamwerk, dat een sterkere nadruk legt op fraudepreventie, klantbescherming, aansprakelijkheidsverdeling en het delen van realtime fraude-informatie. Deze verschuiving heeft directe operationele gevolgen. Deze ontwikkeling sluit ook aan bij bredere trends die worden waargenomen in onderzoeken naar witwaspraktijken en financiële criminaliteit.

Recente analyses van het AMLC: Anti Money Laundering Centre (onderdeel van FIOD) tonen aan dat criminelen steeds vaker gebruikmaken van financiële tussenpersonen, stromannen, complexe eigendomsstructuren en ogenschijnlijk legitieme betalingen om illegaal gedrag te verbergen. In veel gevallen werd verdachte activiteit pas duidelijk toen meerdere zwakke signalen met elkaar in verband werden gebracht en in context werden beoordeeld, in plaats van door middel van één enkele definitieve indicator.⁵

De belangrijkste les is dat effectieve interventie verder moet gaan dan analyse op transactieniveau en moet overgaan naar een bredere beoordeling van gedragsmatige, contextuele en netwerkgebaseerde risico-indicatoren. Financiële instellingen die wachten op sluitend bewijs missen mogelijk kansen om schade te voorkomen, of de onderliggende dreiging nu fraude, witwassen of het faciliteren van criminele activiteiten betreft.

Zoals Nederlandse casestudies over witwasconstructies in de vastgoedsector en financiële tussenpersonen illustreren, kan vroegtijdige herkenning van ongebruikelijke patronen, betrokkenheid van derden, onverklaarde betalingsstructuren en kwetsbaarheid van klanten cruciaal zijn. Zoals gemeld: de uitdaging voor de komende jaren zal zijn om deze lessen te vertalen naar operationele besluitvormingskaders die proportionele interventie ondersteunen vóórdat verliezen optreden, in plaats van uitsluitend te vertrouwen op onderzoek achteraf.

5: Verdachte Transacties als Sleutel tot het Herkennen van Financiële Facilitators." AMLC Anti Money Laundering Centre, 30 Apr. 2026, www.amlc.nl/verdachte-transacties-als-sleutel-tot-het-herkennen-van-financiele-facilitators/

1 Ten eerste wordt de timing van de interventie een primaire maatstaf voor competentie.

De nauwkeurigheid van de detectie is nog steeds belangrijk, maar is op zichzelf niet langer doorslaggevend. Wat het verschil zal maken, is of instellingen vroeg genoeg in het besluitvormingsproces van de klant kunnen ingrijpen om proportionele frictie te introduceren vóórdat geld wordt overgemaakt, in plaats van achteraf technisch correcte waarschuwingen te genereren.

Bedrijven moeten met veel factoren rekening houden als het gaat om proportionele frictie en moeten de mate van frictie óók afstemmen op het risico dat de activiteit met zich meebrengt. Dit geldt voor zowel frauduleuze als legitieme activiteiten: de eisen van consumenten worden steeds meer erkend door autoriteiten en vastgelegd in regelgeving (bijvoorbeeld de Consumer Duty Act in het Verenigd Koninkrijk). Te veel frictie kan leiden tot klantverlies bij legitieme consumenten die onmiddellijke service verwachten. Frictie moet strategisch en verklaarbaar zijn, zowel voor het bedrijf als voor de eindconsument – en natuurlijk moet het bedrijf en de consument beschermd blijven tegen fraude.

2 Ten tweede wordt het vermogen om klantgedrag in context te interpreteren essentiële infrastructuur.

Pure transactiemonitoring kan niet verklaren waarom een klant tegen zijn eigen belangen in handelt. Gedrag in de loop van de tijd, interactiefrequentie en afwijkingen van de persoonlijke norm geven vaak de vroegste signalen van een misdrijf, ruim voordat er geld wordt overgemaakt. Deze signalen kunnen interpreteren vraagt nogal wat van analyses. Zo ontstaat er een voorkeur voor AI-benaderingen die zijn ontworpen om patronen te analyseren in gedrag, intentie, volgorde en afwijking binnen strikt gereguleerde domeinen, in plaats van algemene generatieve systemen.

Tegelijkertijd worden frauduleuze interacties steeds persoonlijker. Door gebruik te maken van open-source data, geleeke informatie en sociale media, stemmen aanvallers hun verhalen steeds vaker af op individuele angsten, motivaties en relaties. Dit verhoogt de slagingskans en vermindert de afhankelijkheid van generieke scripts. Voor banken betekent dit dat veel frauduleuze trajecten nu plausibel, coherent en consistent lijken, juist omdat ze zijn ontworpen rond het leven, het gedrag en de besluitvormingspatronen van de klant.

Klanten willen meestal wel bescherming, maar niet ten koste van een heleboel rompslomp. Onderzoek van FICO toont aan dat 73% van de bankklanten een positievere mening over hun bank zou hebben als deze oplichting in realtime zou stoppen. Tegelijkertijd geven klanten consequent prioriteit aan gemak en snelheid bij financiële transacties. Gedragsonderzoek naar fraudewaarschuwingen bevestigt deze tweestrijd: hoewel de meeste gebruikers waarschuwingen lezen, ondernemen velen er geen actie op, vooral wanneer waarschuwingen generiek, repetitief of slecht in context geplaatst zijn.



Richard Lagerweij ziet dat een structurele verschuiving in de manier waarop bescherming moet werken ontstaan:

“In Nederland hebben de meeste banken al genoeg signalen om te vermoeden dat er iets mis is. De uitdaging zit ‘m niet in de detectie; het gaat om de beslissing wanneer men in actie moet komen. We moeten afstappen van wachten op zekerheid en erkennen wanneer het risico op schade onaanvaardbaar is geworden en vroeg genoeg ingrijpen om de uitkomst te veranderen.”

RICHARD LAGERWEIJ
Product Manager, FICO

De financiële instellingen die het komende jaar succesvol doorkomen, zullen niet de bedrijven zijn waar de meeste waarschuwingen worden gegeven, maar de instellingen die – duidelijk en verdedigbaar – definiëren wanneer gedragssignalen dat ingrijpen rechtvaardigen en hoe bescherming kan worden toegepast zonder het vertrouwen te ondermijnen.

3 Ten derde verschuift de focus van ecosysteem-overschrijdende intelligentie van een streven naar een noodzaak.

Een van de duidelijkste lessen van de recente toename van oplichting is dat social engineering niet binnen de bank begint. Het begint met telefoongesprekken, sms-berichten, berichtenapps en sociale mediaplatformen. Deze realiteit stimuleert nieuwe samenwerkingsmodellen tussen financiële instellingen, sociale-mediaplatformen en telecomproviders.

Deze aanpak is van concept naar praktijk gegaan door een live samenwerking tussen Barclays, Jersey Telecom, FICO en de GSMA (de brancheorganisatie voor de mobiele communicatie-industrie in het Verenigd Koninkrijk). Daarbij werden telecommunicatiesignalen gecombineerd met financiële risico-informatie om social engineering te identificeren terwijl het al gaande was, in plaats van nadat er al verliezen zouden zijn geleden.

Het belang van dit model ligt in het inzicht dat het formaliseert: oplichting is heden ten dage een communicatiegedreven gebeurtenis, voordat het een financiële gebeurtenis wordt. De manipulatie die leidt tot betalingsautorisatie vindt vaak plaats via netwerken die de bank niet of nauwelijks direct kan observeren.

Door risicobeslissingen van de bank te verrijken met telecominformatie kunnen financiële instellingen eerder ingrijpen in de besluitvorming van de klant, wanneer de uitkomsten nog kunnen worden beïnvloed in plaats van alleen achteraf te worden verklaard.



Sarah Cassidy, legt het belang van ecosysteem-overschrijdende kennis uit:

“Banken kunnen de transactiegegevens inzien, terwijl telecombedrijven de manipulatie kunnen zien die eraan voorafgaat aan en die geldactiviteit mogelijk maakt. Wanneer die perspectieven samenkomen, krijgen instellingen eerder context die hen helpt bij het nemen van een besluit. Dat is vaak het verschil tussen het herkennen van een oplichting nadat het geld al is verplaatst en het onderbreken ervan voordat er verliezen optreden.”

SARAH CASSIDY

Fraude-expert, FICO

4 Ten vierde wordt verklaarbaarheid operationeel cruciaal.

Naarmate AI en geavanceerde analyses dieper worden geïntegreerd in het opsporen van fraude en geldezels, moeten financiële instellingen kunnen uitleggen waarom er wel of niet is ingegrepen. Dit is niet langer alleen een vereiste voor model governance. Het zal centraal staan in de regelgeving, de communicatie met klanten en de geschillen die hieruit voortvloeien.



Niets doen is de meest riskante keuze.

5 Ten vijfde wordt het versterken van de positie van medewerkers in de eerste lijn onvermijdelijk.

Fraudeteams kunnen niet effectief opereren als inzichten te laat binnenkomen of verborgen zitten in dashboards. Ze kunnen de gevolgen van oplichting niet vóór zijn, tenzij er beleid en procedures zijn die duidelijk maken wat als voldoende bewijs voor vroegtijdige interventie geldt. Er moet informatie beschikbaar zijn over waar in het proces welke beslissingen worden genomen, of dat nu in digitale klanttrajecten, het callcenter of midden in een betalingsproces is. Technologie moet gebruikers van fraudeteams in staat stellen strategieën te creëren, te simuleren en te implementeren waarmee ze proactief kunnen optreden in de strijd tegen oplichting. Bovendien moet training een continu proces zijn, zodat medewerkers in de eerste lijn de best mogelijke informatie en tools krijgen om op een zinvolle manier met klanten te communiceren, de juiste vragen te stellen en klanten naar de juiste routes te verwijzen.

6 Tot slot is nietsdoen de meest riskante keuze.

Een perfecte gegevensuitwisseling tussen banken, telecombedrijven en sociale-mediaplatformen is op korte termijn onrealistisch. Toezichthouders en het publiek tolereren echter steeds minder situaties waarin instellingen wachten op zekerheid terwijl de schade toeneemt. Vroegtijdig handelen, zelfs met onvolledige informatie, wordt de verwachte norm.



De komende 36 maanden

Misleiding als nieuwe industrie

Over een periode van drie jaar zullen oplichtingspraktijken zich verder professionaliseren en opschalen.



Deepfake-technologie zal een niveau van authenticiteit bereiken waarbij visuele en auditieve signalen niet langer betrouwbare indicatoren van misleiding zijn. Bekende signalen zullen verdwijnen. Oplichtingsinteracties zullen steeds moeilijker te onderscheiden zijn van legitieme communicatie.



Tegelijkertijd zal het model van **scamware-as-a-service** zich sterk verspreiden. Criminele groeperingen zullen scripts, deepfake-tools, werving van geldezels en logica voor het doorsluizen van geld bundelen in modulaire aanbiedingen. De drempel voor andere criminele organisaties om mee te doen zal dalen. Het volume zal toenemen.



Identiteitssystemen zullen daarmee onder aanhoudende druk komen te staan. Naarmate aanvallers experimenteren met het vervalsen of herhalen van biometrische gegevens, zal de afhankelijkheid van statische biometrie afnemen. Authenticatie zal gelaagd, contextueel en continu geëvalueerd moeten worden.



In deze periode wordt **personalisatie** ook geïndustrialiseerd. Taalmodellen en automatisering zullen oplichters in staat stellen op grote schaal gepersonaliseerde verhalen te genereren, die te testen en verder te optimaliseren, waarbij scripts, timing en druktechnieken snel worden aangepast op basis van de reactie van het slachtoffer en institutionele controles. Wat momenteel door ervaren oplichters kan worden bereikt, zal herhaalbaar, meetbaar en continu geoptimaliseerd worden, waardoor social engineering transformeert van een 'ambacht' naar een productiesysteem.



Analistenonderzoek wijst op een belangrijke verdedigingsstrategie in deze periode: **het samenkomen van grafiekanalyse en taalmodellen**. Grafiektechnieken leggen netwerken van tussenpersonen (waaronder geldezel-managers) en gedeelde zwakke punten bloot. Taalmodellen helpen onderzoekers en teams in de eerste lijn om complexe patronen snel te interpreteren. Samen stellen ze banken in staat om te redeneren over netwerken en sequenties in plaats van geïsoleerde gebeurtenissen.

Wat fraude in bredere zin betreft, benadrukt analistenonderzoek ook de noodzaak van bedrijfsbrede configuratie en coördinatie van complexe softwaresystemen op het gebied van data- en risicobeheer. De kloof tussen financiële instellingen die fraude als systemen beschouwen en instellingen die het nog steeds als incidenten behandelen, zal aanzienlijk groter worden.



Erop of eronder: vertrouwen wordt opnieuw opgebouwd of ondermijnd

De belangrijkste vraag over drie jaar is niet: hoe ziet oplichting er dan uit, maar hoe staat het nog met het vertrouwen in de (digitale) financiële wereld?

01



Een plausibele uitkomst is een **hernieuwde focus op vertrouwen**. Naarmate het vertrouwen in zelfbedieningstransacties afneemt, kunnen banken menselijke controles voor risicovolle handelingen opnieuw invoeren. Specialistische teams, verbeterde verificatieprocedures en 'afkoelingstijd' voor transacties zouden opnieuw kunnen verschijnen als het vertrouwen zich stabiliseert.

02



Een andere mogelijkheid is **autonome verdediging**, waarbij systemen redeneren over gedrag, taal, netwerken en tijd om proportionele interventies te genereren met minimale menselijke vertraging, terwijl mensen verantwoordelijk blijven.

03

Een ander, somberder scenario is **genormaliseerde schade**, waarbij verliezen door oplichting worden geaccepteerd als de prijs voor digitaal gemak en waarbij het vertrouwen langzaam, maar steeds verder afneemt.

Tegen 2030 verwachten we wereldwijd verschillende benaderingen en uitkomsten op dit gebied, gebaseerd op uiteenlopende prioriteiten, dreigingsniveaus, technologische volwassenheidsniveaus en meer. Welke weg de overhand krijgt in Nederland, hangt af van de beslissingen die nu worden genomen inzake vroegtijdige interventie, technologische modernisering, de coördinatie daaromheen en de bereidheid om te handelen voordat absolute zekerheid bestaat.

De belangrijkste opdracht voor fraudemanagers



Voor fraudeafdelingen in Nederland is de taak een flink stuk uitgebreid. Het draait niet langer om het stoppen van frauduleuze transacties. Het gaat erom of men op cognitieve manipulatie kan anticiperen, of men eerder durft in te grijpen, of het vertrouwen op grote schaal beschermd wordt, zelfs wanneer dit ongemakkelijk of onzeker is.



In Europese markten waar digitale betalingen, mobiel bankieren en realtime overboekingen de norm zijn geworden, is **klantgedrag het cruciale drukpunt in fraudepreventie**. De klantervaring is steeds belangrijker in deze strijd. De keuzes die de komende jaren worden gemaakt over vroegtijdige interventie, coördinatie tussen ecosystemen en het verantwoord gebruik van geavanceerde analyses, zullen bepalen of het vertrouwen in digitale financiële systemen in Nederland en in Europa verder zal toenemen.



**Kom meer te weten over het beschermen van
consumenten tegen oplichting**

www.fico.com/en/solutions/scams-protection

**Ontdek de innovaties van FICO op het gebied van
fraudebestrijding voor ondernemingen**

**[www.fico.com/en/solutions/enterprise-fraud-
innovations](https://www.fico.com/en/solutions/enterprise-fraud-innovations)**

Neem contact op

<https://nl.fico.com/>

