Fraudebarometer 2025 van Nederland



KPMG Nederland

—

Oktober 2026

KPMG. Make the difference.

Van veroordelingspatronen naar gerichte actie

Wat de inzichten uit de Fraudebarometer 2025 betekenen voor de prioriteiten rondom fraude, integriteit en compliance in 2026

De KPMG Fraudebarometer biedt een unieke kijk op witteboordencriminaliteit in Nederland door het analyseren van mediaberichten over zaken die in 2025 tot een uitspraak of schikking van een Nederlandse rechtbank hebben geleid. Frauduleuze verslaggeving en verduistering vormen het grootste deel van de veroordelingen. De daders variëren van externe individuen en medewerkers tot georganiseerde criminele groepen. De bevindingen laten zien dat financiële criminaliteit een brede groep belanghebbenden raakt, waaronder bedrijven, overheidsinstanties en de maatschappij als geheel.

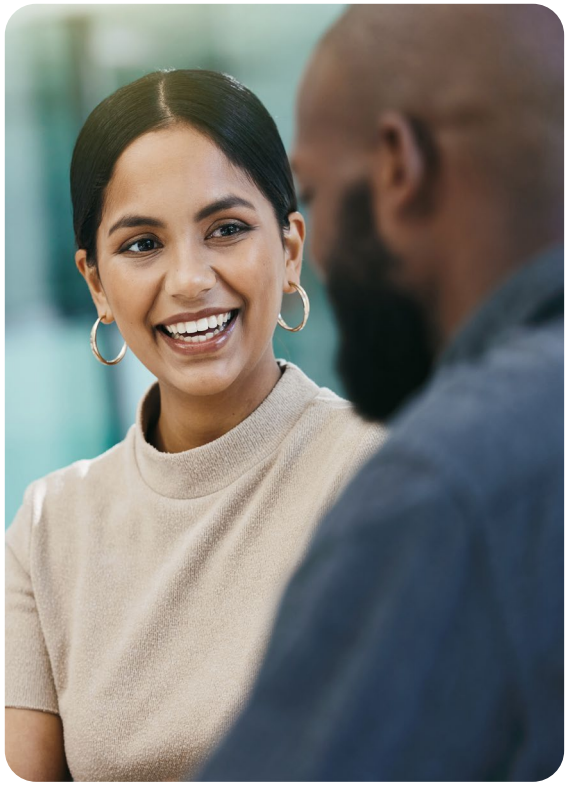
De uitdaging van interne daders

Hoewel externe individuen het grootste deel van de veroordeelde daders vormen, blijkt uit de bevindingen dat een aanzienlijk deel van de zaken medewerkers en personen in vertrouwensposities betreft. Organisaties staan dus niet alleen bloot aan dreigingen van buitenaf, maar ook aan risico's vanuit de eigen organisatie.

Medewerkers hebben vaak toegang tot gevoelige informatie, systemen en financiële middelen, wat kansen biedt om wangedrag te plegen of te faciliteren. Naast externe fraudepreventie zijn daarom beheersmaatregelen voor interne risico's nodig, zoals functiescheiding, monitoring en effectief toezicht. Een sterke integriteitscultuur en het stimuleren van meldingen helpen bovendien om risico's vroegtijdig te signaleren en aan te pakken.

Een samenhangende aanpak

De verscheidenheid aan delicten, daders en slachtoffergroepen laat zien dat risico's van financiële criminaliteit zelden op zichzelf staan.



Fraude, integriteitsschendingen en witwasrisico's overlappen vaak, terwijl dezelfde personen, netwerken of tekortkomingen in de beheersing meerdere vormen van wangedrag mogelijk kunnen maken. Een geïsoleerde aanpak kan daardoor leiden tot blinde vlekken en versnipperde reacties.

Een meer geïntegreerde aanpak vergroot de weerbaarheid. Door governance, risicomanagement, interne beheersing, onderzoeken en meldmechanismen op elkaar af te stemmen, ontstaat een volledig beeld van het risicolandschap. Dit versterkt het toezicht, maakt eerdere detectie mogelijk en ondersteunt een gecoördineerde reactie binnen de organisatie.

Vooruitblik

Naarmate organisaties verder digitaliseren en AI-technologieën toepassen, zullen fraudepatronen mee evolueren en ontstaan er nieuwe uitdagingen voor preventie en detectie. Tegelijkertijd bieden ontwikkelingen in data-analyse en AI sterke mogelijkheden om verdacht gedrag eerder te herkennen, fraudedetectie te versterken en onderzoeken effectiever uit te voeren.



Leonie Stolk
Partner
Hoofd Forensic NL

"Financiële criminaliteit beperkt zich zelden tot één risicodomein.

Gezien de complexiteit van het huidige risicolandschap is het voor organisaties essentieel om fraude-, integriteits- en compliance-risico's niet langer afzonderlijk te benaderen, maar geïntegreerd aan te pakken.

Vooruitkijkend, brengt AI niet alleen nieuwe risico's en kansen met zich mee, maar het verandert ook hoe organisaties financiële criminaliteit kunnen voorkomen, detecteren en aanpakken."

© 2026 KPMG Advisory N.V., een naamloze vennootschap en lid van het KPMG-netwerk van zelfstandige ondernemingen die verbonden zijn aan KPMG International Limited, een Engelse entiteit. Alle rechten voorbehouden.

Fraudebarometer 2025

Kerninzichten

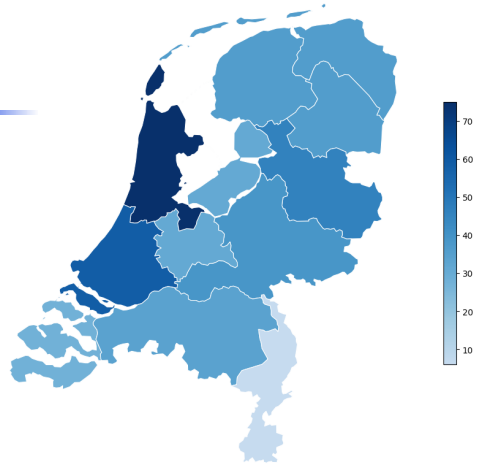
Het landschap van witteboordencriminaliteit in Nederland in 2025

De KPMG Forensic Fraudebarometer omvat uitsluitend witteboordencriminaliteit die in 2025 tot veroordelingen door Nederlandse rechters heeft geleid

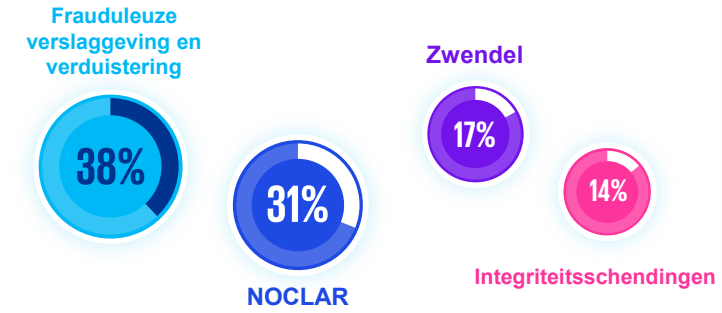
38%

van de rechtbankzaken komt uit de provincies Noord- en Zuid-Holland, samen vertegenwoordigen ze de grootste regionale concentratie van veroordeelde zaken.

Veroordeelde zaken per regio



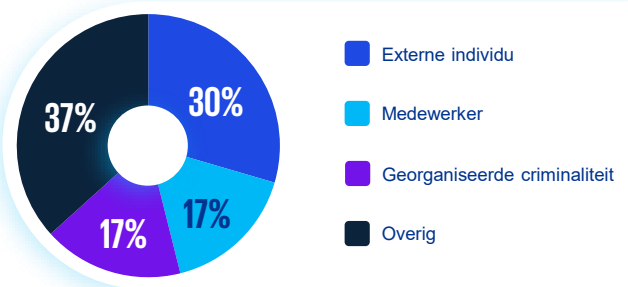
Verdeling van veroordelingen per domein



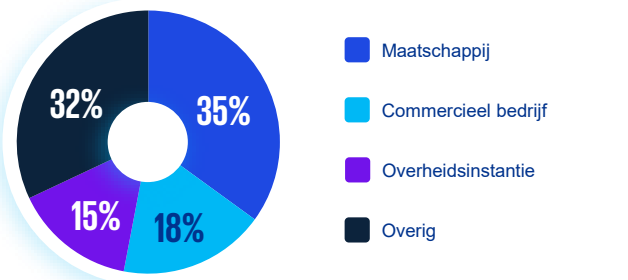
Meest voorkomende delicten onder veroordelingen



Externe individuen, medewerkers en georganiseerde criminaliteit vormen 64% van de veroordeelde personen



Maatschappij, commerciële bedrijven en overheidsinstanties vormen 68% van de slachtoffers



n=447 | Door afrondingsverschillen tellen percentages mogelijk niet altijd op tot 100%. Dit geldt voor alle volgende grafieken en figuren in dit rapport.

© 2026 KPMG Advisory N.V., een naamloze vennootschap en lid van het KPMG-netwerk van zelfstandige ondernemingen die verbonden zijn aan KPMG International Limited, een Engelse entiteit. Alle rechten voorbehouden.

Inhoud

01	De diversiteit van witteboordencriminaliteit	05
02	Verdieping: ‘frauduleuze verslaggeving en verduistering’	09
03	Verdieping: ‘NOCLAR’	11
04	Verdieping: ‘zwendel’	13
05	Verdieping: ‘integriteitsschendingen’	15
06	Van inzichten naar actie	17



© 2026 KPMG Advisory N.V., een naamloze vennootschap en lid van het KPMG-netwerk van zelfstandige ondernemingen die verbonden zijn aan KPMG International Limited, een Engelse entiteit. Alle rechten voorbehouden.

De diversiteit van witteboordencriminaliteit

Met Nederlandse media als primaire bron biedt de Fraudebarometer inzicht in witteboordencriminaliteit in Nederland. Alleen zaken die in 2025 leidden tot een formele uitspraak of schikking van een Nederlandse rechter zijn meegenomen. De analyse biedt een unieke kijk op hoe financiële en integriteit gerelateerde criminaliteit zich in de praktijk manifesteert en binnen het Nederlandse rechtssysteem wordt aangepakt.

De Fraudebarometer beslaat een breed spectrum aan financiële en integriteit gerelateerde delicten die aansluiten op de type misstanden die wij regelmatig in ons werk tegenkomen. Deze omvatten onder meer delicten zoals verduistering, witwassen en jaarrekeningfraude. Ook niet-financiële vormen van wangedrag zijn meegenomen, waaronder wangedrag op de werkvloer, belangenverstrengeling en machtsmisbruik. Dit weerspiegelt de diversiteit aan frauderisico's en veroordelingen in Nederland.

In 2025 publiceerde KPMG Global het *Global Profile of the Fraudster**, met inzichten in het profiel van de typische fraudeur. De Fraudebarometer vult dit aan met een Nederlands perspectief op gepleegde fraude en de betrokken belanghebbenden.

Welkom bij de Nederlandse Fraudebarometer 2025. De Fraudebarometer is een initiatief van KPMG Forensic, onderdeel van KPMG Advisory N.V. (hierna: 'KPMG').

Deze publicatie biedt belangrijke inzichten in het Nederlandse fraudelandschap van 2025, waaronder de prevalentie van verschillende fraudetypen, groepen daders en slachtoffers en opgelegde straffen. Binnen dit onderzoek zijn 31 subtypen van integriteit en fraude gerelateerde criminaliteit vastgesteld. Vanwege deze diversiteit zijn ze ondergebracht in vier hoofddomeinen:

Frauduleuze verslaggeving en verduistering

Zaken waarin toevertrouwde activa, middelen of informatie worden misbruikt voor financieel gewin. Dit domein omvat onder meer verduistering, valsheid in geschrifte, belastingfraude en manipulatie van financiële of administratieve vastleggingen.

Zwendel

Zaken waarin slachtoffers door misleiding of manipulatie geld, activa of andere voordelen afhandig worden gemaakt. Dit omvat uiteenlopende vormen van oplichting, zoals fraude onder valse voorwendselen, beleggingsfraude, onlinefraude en cyber gerelateerde misleiding.

NOCLAR (Non-Compliance with Laws en Regulations)

Zaken omtrent overtredingen van wettelijke vereisten, zoals witwassen, sanctieschendingen, omkoping, corruptie en andere compliance-schendingen. Vaak gaat het om het verhullen van illegale opbrengsten of het niet naleven van wettelijke verplichtingen.

Integriteitsschendingen

Zaken omtrent gedrag dat ethische normen, professionele verantwoordelijkheden of de integriteit van organisaties ondermijnt. Voorbeelden zijn machtsmisbruik, belangenverstrengeling, schenden van ambtsgeheim, wangedrag op het werk en andere vormen van grensoverschrijdend gedrag.

Het rapport geeft een overzicht van actuele risico's en patronen binnen deze domeinen, waarbij in hoofdstukken 2 tot en met 5 een verdieping per domein wordt gegeven. Zo worden veranderende risico's en kwetsbaarheden voor organisaties, publieke instellingen en individuen zichtbaar. Deze inzichten helpen belanghebbenden te begrijpen hoe fraude wordt gepleegd, wanneer zij aan belangrijke risico's blootstaan en welke preventieve maatregelen nodig kunnen zijn.

Neem gerust contact met ons op als u meer wilt weten over de uitvoering van dit onderzoek.

© 2026 KPMG Advisory N.V., een naamloze vennootschap en lid van het KPMG-netwerk van zelfstandige ondernemingen die verbonden zijn aan KPMG International Limited, een Engelse entiteit. Alle rechten voorbehouden.

* Zie voor meer informatie de Global Profiles of the Fraudster

De diversiteit van witteboordencriminaliteit

Verdeling van veroordelingen

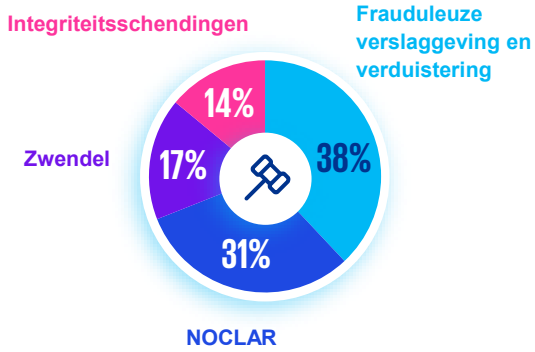
In totaal werden in Nederlandse media 447 unieke zaken geïdentificeerd, waarbij elke veroordeelde persoon geldt als een afzonderlijke zaak; een delict met twee veroordeelden telt dus als twee zaken.

De verdeling van de veroordelingen laat zien dat **frauduleuze verslaggeving en verduistering** (38%) en **NOCLAR** zaken (31%) de vaakst veroordeelde vormen van witteboordencriminaliteit zijn. Waar het eerste domein onder meer valsheid in geschrifte en verduistering omvat, bevat het tweede witwassen en andere compliance-schendingen. De prevalentie van deze delicten onderstreept het belang van sterke financiële beheersmaatregelen, effectieve transactiemonitoring en robuuste compliance frameworks.

Tegelijkertijd tonen **zwendel**-gerelateerde delicten, waaronder oplichting en cyberfraude, het belang aan van effectieve cybersecurity, klantbescherming en bewustzijn van externe dreigingen.

Integriteitsschendingen (zoals machtsmisbruik en grensoverschrijdend gedrag) komen minder vaak voor in rechtszaken. Uit onze ervaring blijkt dat integriteitsschendingen vaak intern worden afgehandeld in plaats van via juridische procedures. Preventie vraagt om een sterke organisatiecultuur, duidelijke governance en effectieve meldmechanismen, die ook risico's van interne actoren helpen beperken.

Verdeling van veroordelingen over domeinen in Nederland



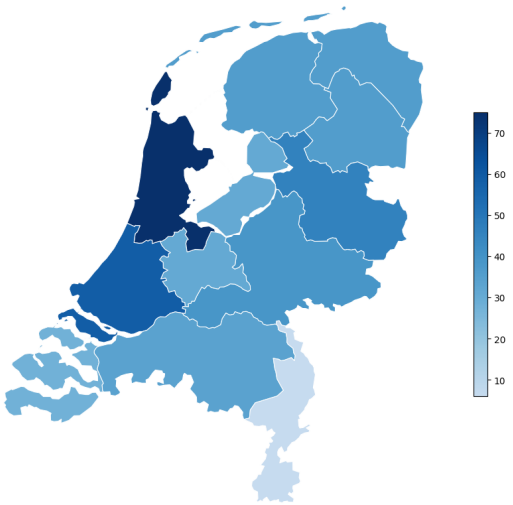
Geografische inzichten

De aanwezigheid van alle vier de domeinen onderstreept het belang van een geïntegreerde aanpak, waarin financiële, compliance- en integriteitsmaatregelen samenkomen om de risico's van witteboordencriminaliteit effectief te beheersen.

Op basis van de rechtbanklocatie is de geografische spreiding van veroordelingen geanalyseerd*. **Noord-Holland** en **Zuid-Holland** vertegenwoordigen samen 38% van de rechtbankzaken, wat samenhangt met hun hogere bevolkingsdichtheid en economische activiteit. De verdeling van veroordelingen over de vier domeinen komt hier sterk overeen met het landelijke beeld.

Daarentegen kennen **Gelderland** en **Overijssel**, samen goed voor 24% van de rechtbankzaken, relatief meer zwendel gerelateerde veroordelingen (24%) en minder NOCLAR-veroordelingen (23%).

Geografische verdeling van veroordeelde zaken in Nederland



* De geografische verdeling betreft uitsluitend zaken waarin Nederlandse rechtbanken een veroordeling uitspraken. Zaken bij hogere rechterlijke instanties, zoals gerechtshoven en de Hoge Raad, en uitspraken van tuchtrechtelijke instanties zijn hierin niet opgenomen.

© 2026 KPMG Advisory N.V., een naamloze vennootschap en lid van het KPMG-netwerk van zelfstandige ondernemingen die verbonden zijn aan KPMG International Limited, een Engelse entiteit. Alle rechten voorbehouden.

Daders en slachtoffers

Witteboordencriminaliteit kent een breed scala aan daders en een even diverse groep slachtoffers.

Wat betreft de daders zijn **externe individuen** verantwoordelijk voor 30% van de zaken en zijn daarmee een belangrijke aanjager van witteboordencriminaliteit. Bijna de helft van deze zaken houdt verband met witwassen (45%) en gaat doorgaans niet gepaard met andere veroordelingen binnen de scope vallen. Dit kan erop wijzen dat zij vaker geïsoleerd opereren, mogelijk met banden met georganiseerde criminele netwerken die in deze barometer of in rechterlijke uitspraken niet volledig zichtbaar zijn. Hun voornaamste slachtoffers zijn **de maatschappij** of **commerciële bedrijven**.

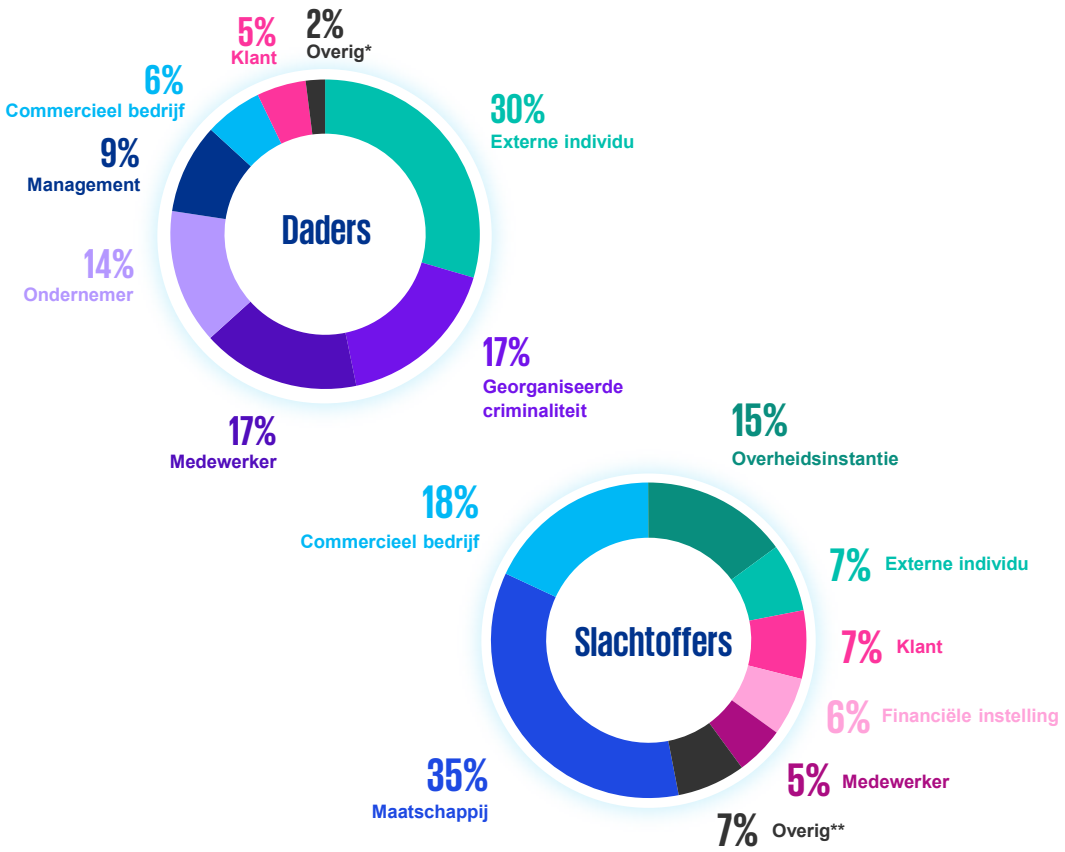
Georganiseerde criminaliteit vertegenwoordigt 17% van de daders. Dit laat zien dat een aanzienlijk deel van de wittenboordencriminaliteit niet incidenteel is, maar gestructureerd en professioneel gecoördineerd. In de praktijk probeerden deze daders vaak de herkomst te verhullen van middelen uit drugscriminaliteit of andere delicten buiten de scope van de barometer. In zaken met georganiseerde criminaliteit wordt **de maatschappij** doorgaans als voornaamste slachtoffer aangemerkt, wat de brede en indirecte impact op het financiële stelsel en het publieke vertrouwen weerspiegelt.

Medewerkers vormen eveneens 17% van de daders. Dit benadrukt dat frauderisico niet alleen van buitenaf komt, maar ook voortkomt uit insider risk binnen organisaties. Medewerkers worden vooral in verband gebracht met verduistering (25%) en richten zich doorgaans op hun eigen organisatie (zoals **commerciële** en **niet-commerciële instellingen** en **overheidsinstanties**) en in enkele gevallen op haar **klanten**. Een sterke beheersingsomgeving, met onder meer functiescheiding en voortdurende bewustwording, blijft daarom essentieel om insider risk te beperken.

Ondernemers zijn verantwoordelijk voor 14% van de zaken. Zij worden het vaakst veroordeeld voor valsheid in geschrifte (28%) en in mindere mate voor witwassen, oplichting en belastingfraude. **Overheidsinstanties** zijn de voornaamste slachtoffers, wat de blootstelling van publieke instellingen aan financiële verslaggevings- en belastingovertredingen benadrukt.

In lijn met KPMG's *Global Profile of the Fraudster** publicatie tonen deze inzichten aan dat organisaties worden geconfronteerd met frauderisico's vanuit zowel interne als externe actoren. Beheersing vraagt om effectieve controles, continue monitoring van rollen en toegangsniveaus en blijvende aandacht voor het gestructureerde en gecoördineerde karakter van bepaalde fraudepatronen.

Verdeling van daders en slachtoffers van witteboordencriminaliteit



* 'Overig' omvat de volgende typen daders: financiële instelling (0,9%), overheidsinstantie (0,7%) en niet-commerciële instelling (0,4%).
** 'Overig' omvat de volgende typen slachtoffers: ondernemer (2,9%), niet-commerciële instelling (2,6%) en management (1,2%).

© 2026 KPMG Advisory N.V., een naamloze vennootschap en lid van het KPMG-netwerk van zelfstandige ondernemingen die verbonden zijn aan KPMG International Limited, een Engelse entiteit. Alle rechten voorbehouden.

* Zie voor meer informatie de Global Profiles of the Fraudster

Straffen

De opgelegde straffen onderstrepen de ernst waarmee financiële en integriteit gerelateerde delicten worden behandeld.

Financiële sancties, waaronder boetes, schadevergoedingen en verbeurdverklaringen, vormen een belangrijk onderdeel van deze zaken. De totale waarde ervan verschilt sterk per type delict, zowel absoluut als in verhouding tot het aantal zaken. Hoewel deze bedragen compensatie- en verhaalsmaatregelen omvatten, zijn niet-verhaalde verliezen en niet-monetair geconfisqueerde activa hierin niet meegenomen. De bedragen vormen daarom geen directe afspiegeling van de totale schade.

Frauduleuze verslaggeving en verduistering zaken vertegenwoordigen met circa EUR 210 miljoen het grootste aandeel in de financiële sancties. Dit sluit aan bij het feit dat dit domein het grootste aandeel van alle zaken vertegenwoordigt (38%). Hoewel het totaal mede wordt bepaald door het hoge aantal zaken, blijft ook de financiële impact per zaak aanzienlijk vergeleken met andere domeinen. De combinatie van een hoog aantal zaken en substantiële financiële sancties toont aan dat traditionele fraudevormen een belangrijk risico voor organisaties blijven vormen.

Zwendel vertegenwoordigt weliswaar een kleiner aandeel van het totale aantal zaken (17%), maar heeft een relatief hoge totale financiële impact van circa EUR 109 miljoen. Dit wijst erop dat individuele zwendelzaken vaak aanzienlijke financiële schade met zich meebrengen, waardoor de verliezen per incident hoog kunnen oplopen. Externe frauderisico's, waaronder oplichting, identiteitsfraude en computervredebreuk, blijven daarom een belangrijk risico voor organisaties.

NOCLAR-zaken vertegenwoordigen 31% van alle zaken, maar leiden tot een aanzienlijk lagere totale waarde aan financiële sancties, namelijk circa EUR 32 miljoen*. Dit wijst erop dat financiële compensaties in deze zaken, ondanks hun frequentie, relatief beperkt blijven. Tegelijkertijd leiden witwaszaken vaker tot (langere) celstraffen (48%), wat de ernst van deze delicten bij niet-financiële sanctionering weerspiegelt. Organisaties die onder anti-witwasregelgeving (AML) vallen, blijven blootgesteld aan aanzienlijke toezichts- en handhavingsrisico's, aangezien non-compliance naast financiële sancties ook ernstige juridische gevolgen kan hebben voor betrokken personen. Dit benadrukt het belang van effectieve due diligence, transactiemonitoring en tijdige escalatie van verdachte activiteiten.

Integriteitsschendingen, goed voor 14% van de zaken, kennen met circa EUR 22 miljoen de laagste totale financiële sancties. Dit kan samenhangen met de aard van deze zaken, die niet altijd leiden tot grote kwantificeerbare financiële schade. Integriteitsschendingen brengen voor organisaties echter vaak aanzienlijke reputatierisico's met zich mee, die kunnen leiden tot verscherpt toezicht door toezichthouders en hoge kosten voor intern onderzoek of herstelmaatregelen.

Organisaties hebben daarom baat bij een sterke ethische cultuur, ondersteund door duidelijke beleidsregels en toegankelijke meldkanalen.

De data toont dat zowel de frequentie van zaken als het type en de omvang van sancties sterk verschillen per delict domein. Organisaties lopen uiteenlopende financiële, toezichts-, juridische en reputatierisico's, waardoor een risicogebaseerde aanpak van fraude- en compliancebeheersing essentieel is.

* Deze waardes betreffen uitsluitend Nederlandse rechtszaken en omvatten geen internationale boetes. De waardes weerspiegelen uitsluitend de bedragen die zijn vermeld in de media-artikelen binnen de scope van het onderzoek, waardoor mogelijk niet alle opgelegde financiële sancties zijn meegenomen.

Financiële sancties



© 2026 KPMG Advisory N.V., een naamloze vennootschap en lid van het KPMG-netwerk van zelfstandige ondernemingen die verbonden zijn aan KPMG International Limited, een Engelse entiteit. Alle rechten voorbehouden.

Verdieping: 'frauduleuze verslaggeving en verduistering'

Veroordelingen voor frauduleuze verslaggeving en verduistering

We identificeerden 186 unieke zaken met een veroordeling binnen het domein frauduleuze verslaggeving en verduistering.

Dit domein omvat uiteenlopende veroordelingen, van valsheid in geschrifte en belastingfraude tot faillissements- en uitkeringsfraude. Deze delicten staan zelden op zichzelf. In 42% van de zaken werden daders veroordeeld voor een combinatie van witteboordendelicten. De meeste combinaties overstijgen meerdere domeinen, zoals valsheid in geschrifte uit het domein Frauduleuze verslaglegging en verduistering in combinatie met oplichting uit het domein Zwendel. Het grote aandeel veroordelingen voor meerdere delicten wijst erop dat witteboordencriminaliteit vaak via verweven constructies wordt gepleegd.

Valsheid in geschrifte is het duidelijkste voorbeeld van deze verwevenheid. Met 44% van de veroordelingen is dit niet alleen het meest voorkomende delict, maar lijkt het ook vaak grotere fraudeconstructies mogelijk te maken. De meest voorkomende combinaties verbinden valsheid in geschrifte met oplichting, witwassen en verduistering. Vervalste contracten, jaarrekeningen en andere documenten kunnen zo worden gebruikt om belanghebbenden te misleiden en illegale opbrengsten te verhullen.

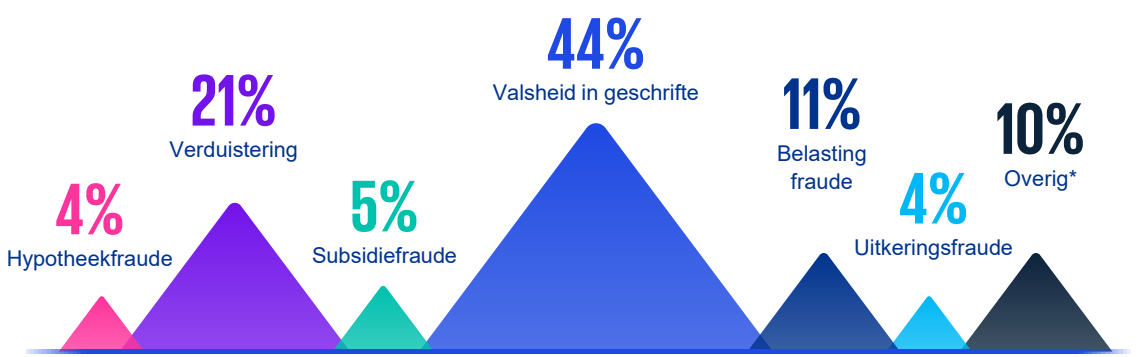
Door de voortdurende ontwikkelingen op het gebied van AI worden vervalste documenten steeds moeilijker te herkennen. Dit benadrukt niet alleen het belang van effectieve controles en goedkeuringsprocessen, maar ook van AI-ondersteunde detectiemaatregelen om steeds geavanceerdere dreigingen tijdig te identificeren.

Verduistering (21%), de op één na meest voorkomende veroordeling, komt eveneens vaak voor in combinatie met andere delicten, met name valsheid in geschrifte. Verduistering is hoofdzakelijk een intern risico en ontstaat vaak wanneer iemand vertrouwde toegang heeft tot geld of activa. Onvoldoende functiescheiding en beperkt toezicht kunnen de kans op verduistering vergroten.

Daarentegen komt **belastingfraude** (11%) vaker als zelfstandig delict voor. Belastingfraude kan daders een oneerlijk concurrentievoordeel geven, overheidsinkomsten verlagen en het vertrouwen in het economische stelsel ondermijnen. Dit risico kan ontstaan wanneer fiscale posities, transacties of verslaggeving onvoldoende worden getoetst of gecontroleerd.

Deze bevindingen laten zien dat risico's elkaar kunnen versterken en niet los van elkaar moeten worden bekeken. Zonder adequate beheersing kunnen deze risico's leiden tot overtredingen van wet- en regelgeving, reputatieschade, aanzienlijke financiële verliezen en verminderd vertrouwen van publiek en belanghebbenden. De bevindingen onderstrepen ook het belang van geïntegreerd frauderisicomanagement, aangezien zwakheden op één gebied ruimte kunnen bieden aan bredere en complexere fraudeconstructies.

Verdeling van veroordelingen voor frauduleuze verslaggeving en verduistering



* 'Overig' omvat de volgende subtypen: declaratiefraude (3,0%), faillissementsfraude (3,0%), verzekeringsfraude (2,2%), jaarrekeningfraude (1,3%) en beleggingsfraude (0,9%).

© 2026 KPMG Advisory N.V., een naamloze vennootschap en lid van het KPMG-netwerk van zelfstandige ondernemingen die verbonden zijn aan KPMG International Limited, een Engelse entiteit. Alle rechten voorbehouden.

De daders

Uit de analyse van de 186 zaken blijkt dat fraude door uiteenlopende actoren kan worden gepleegd, waarbij het daderprofiel zowel de aard van het delict als het type slachtoffer beïnvloed.

Ondernemers, goed voor 25% van de daders, worden vooral in verband gebracht met valsheid in geschrifte en belastingfraude, gericht tegen overheidsinstanties, commerciële bedrijven en klanten. Risico's kunnen dus zowel binnen organisaties als via externe zakelijke relaties ontstaan, wat het belang benadrukt van effectieve controles op documentatie en financiële verslaggeving, met name wanneer individuen over een grote mate van autonomie beschikken.

Medewerkers (20%) en **management** (12%) zijn het vaakst betrokken bij verduistering en valsheid in geschrifte. Deze delicten komen voor bij overheidsinstanties en commerciële en niet-commerciële instellingen, en laten zien hoe toegang, bevoegdheden en proceskennis kunnen worden misbruikt voor persoonlijk gewin.

Georganiseerde criminaliteit (12%) en **externe individuen** (9%) worden vooral in verband gebracht met valsheid in geschrifte en belastingfraude, vaak gericht tegen commerciële bedrijven en overheidsinstanties. Frauderisico's kunnen dus ook buiten de organisatie ontstaan. Dit benadrukt het belang van gedegen due diligence en monitoring van contacten met derden.

De slachtoffers

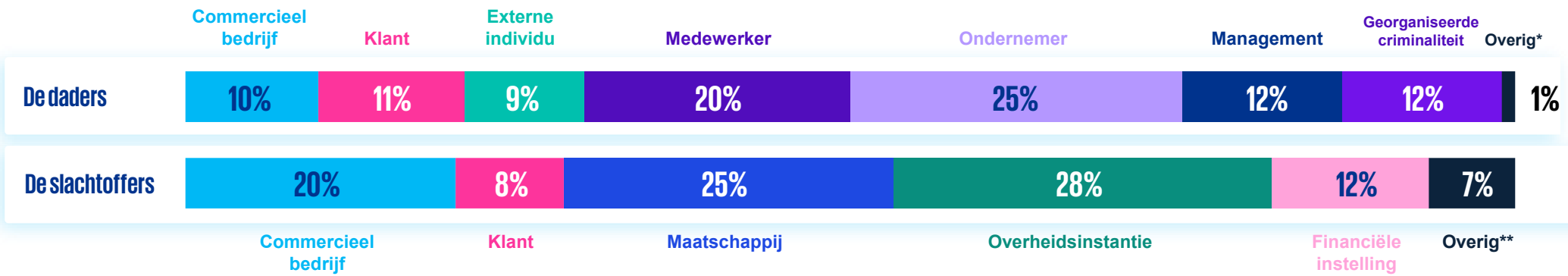
Vanuit het perspectief van de slachtoffers vormen overheidsinstanties de grootste groep, gevolgd door de maatschappij, commerciële bedrijven en financiële instellingen. In 25% van de zaken is meer dan één type slachtoffer betrokken.

Overheidsinstanties vormen 28% van de slachtoffers en worden vaak getroffen door belasting-, subsidie- en uitkeringsfraude. Deze delicten raken ook indirect de maatschappij: belastingfraude beperkt publieke inkomsten, terwijl subsidie- en uitkeringsfraude de uitgaven onterecht verhogen. Daardoor blijven minder middelen over voor publieke prioriteiten.

Commerciële bedrijven vormen 20% van de slachtoffers en worden vooral getroffen door interne daders, zoals medewerkers en management, met name via verduistering en valsheid in geschrifte. Dit onderstreept het belang van de beheersing van insider risk, waarbij toegang, bevoegdheden en kennis van interne processen ruimte kunnen bieden voor ongewenst gedrag.

Financiële instellingen vormen 12% van de slachtoffers en worden getroffen door verschillende typen daders, waaronder hun eigen klanten via hypotheekfraude en valsheid in geschrifte. Dit benadrukt de blijvende noodzaak van cliëntenonderzoek en documentverificatie.

Verdeling van daders en slachtoffers binnen het frauduleuze verslaggeving en verduistering domein



* 'Overig' omvat de volgende typen daders: financiële instelling (0,5%) en niet-commerciële instelling (0,5%). ** 'Overig' omvat de volgende typen slachtoffers: externe individu (3,3%) en niet-commerciële instelling (3,3%).

© 2026 KPMG Advisory N.V., een naamloze vennootschap en lid van het KPMG-netwerk van zelfstandige ondernemingen die verbonden zijn aan KPMG International Limited, een Engelse entiteit. Alle rechten voorbehouden.

Verdieping: 'NOCLAR'

NOCLAR veroordelingen

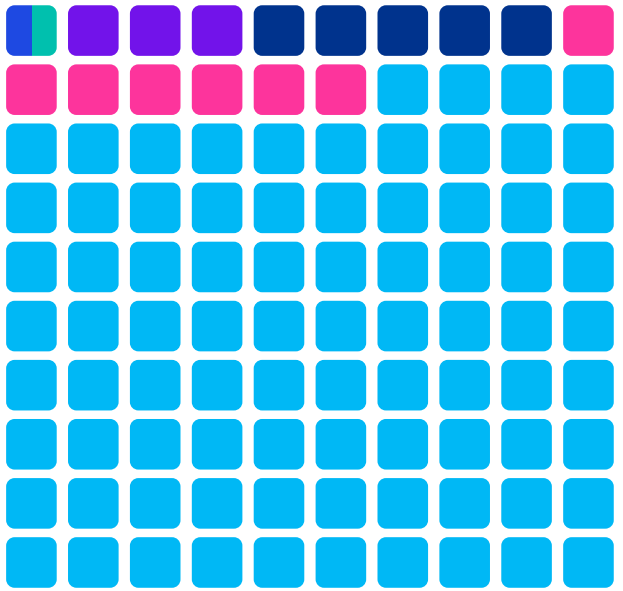
In totaal werden 181 unieke zaken vastgesteld binnen het NOCLAR domein, waarbij witwassen veruit het meest voorkomende delict was (155 veroordelingen).

In ruim een kwart van de zaken komt **witwassen** voor in combinatie met andere witteboordendelicten, vooral valsheid in geschrifte en oplichting. Dit wijst op de rol van witwassen als verhullingslaag binnen bredere constructies, waarbij vervalste documenten worden gebruikt om een schijn van legitimiteit te creëren en oplichting illegale opbrengsten genereert. Hoewel de meeste witwasveroordelingen binnen dit rapport op zichzelf staan, blijkt uit de zaken dat witwassen vaak verband houdt met gronddelicten buiten de scope van deze barometer, zoals drugshandel. Witwassen wordt ook sterk geassocieerd met celstraffen, waarbij de langste opgelegde straf tien jaar bedroeg. Voor financiële instellingen blijven gedegen cliëntenonderzoek, transactiemonitoring en escalatieprocedures voor ongebruikelijke activiteiten belangrijke waarborgen tegen misbruik van financiële dienstverlening. Het niet detecteren van dergelijke activiteiten kan aanzienlijke gevolgen hebben op toezichts-, financieel en reputatiegebied.

Daarentegen zijn **andere compliance-schendingen** (7%) vrijwel uitsluitend op zichzelf staande delicten. Waar de andere NOCLAR-categorieën onderliggende delicten betreffen, gaat deze categorie over het niet naleven van wettelijke verplichtingen, zoals tekortkomingen in AML-controles, fraudedetectie, toezicht en governance. In ongeveer de helft van deze zaken worden bedrijven als dader aangemerkt, waardoor boetes vaak worden opgelegd, terwijl individuele aansprakelijkheid vaker leidt tot celstraffen. Effectief beleid, toezicht en naleving van regelgeving blijven belangrijke waarborgen tegen dergelijke incidenten.

Omkoping (5%) en **corruptie** (3%) komen minder vaak voor, maar staan zelden op zichzelf. Ze hangen vaak samen met valsheid in geschrifte en computervredebreuk en kennen doorgaans meerdere daders. Organisaties moeten daarom verder kijken dan afzonderlijke incidenten en rekening houden met de rol van derde partijen, interne invloed en misbruik van systemen.

Verdeling van NOCLAR veroordelingen



- 0.5% Sancties
- 0.5% Terrorismefinanciering
- 3% Corruptie
- 5% Omkoping
- 7% Andere compliance-schendingen
- 84% Witwassen

Tot slot bevat de dataset een beperkt aantal zaken rond sancties en **terrorismefinanciering**. Ondanks hun geringe aantal laten deze zaken zien dat beide risico's relevant blijven en onderdeel moeten blijven uitmaken van AML-, sanctie- en screeningkaders, gezien de mogelijk verstrekkende gevolgen.

© 2026 KPMG Advisory N.V., een naamloze vennootschap en lid van het KPMG-netwerk van zelfstandige ondernemingen die verbonden zijn aan KPMG International Limited, een Engelse entiteit. Alle rechten voorbehouden.

De daders

Binnen dit domein zijn externe individuen en georganiseerde criminaliteit samen verantwoordelijk voor 71% van de veroordeelde zaken. Tegelijkertijd blijft intern risico eveneens aanzienlijk: ondernemers, medewerkers en management zijn samen verantwoordelijk voor 24% van de zaken.

Externe individuen (40%) en **georganiseerde criminaliteit** (31%) houden vrijwel uitsluitend verband met witwaszaken. Dit suggereert dat witwassen niet alleen via gestructureerde criminele netwerken, maar ook regelmatig zelfstandig wordt gepleegd. Dit kan wijzen op een lage instapdrempel, waarbij individuen optreden als facilitators of tussenpersonen (zoals geldezels of kleinschalige actoren), terwijl georganiseerde groepen complexere constructies aansturen.

Ondernemers (11%) worden eveneens vooral in verband gebracht met witwassen, wat kan wijzen op een rol als katvanger om illegale geldstromen te verhullen. Hun betrokkenheid bij omkoping en andere compliance-schendingen, die vooral commerciële bedrijven en de maatschappij treffen, benadrukt het belang van gedegen due diligence in zakelijke relaties en effectief compliancetoezicht.

Medewerkers (7%) en **management** (6%) komen minder vaak voor binnen dit domein, maar zijn bij betrokkenheid vaker gekoppeld aan omkoping en corruptie. Dit suggereert dat toegang, bevoegdheden en invloed binnen organisaties een belangrijke rol kunnen spelen bij deze delicten, die voornamelijk commerciële bedrijven raken.

De slachtoffers

De maatschappij (64%) vormt de grootste slachtoffergroep, mede door het grote aandeel witwaszaken en de brede impact op de financiële integriteit, marktstabiliteit en publiek vertrouwen.

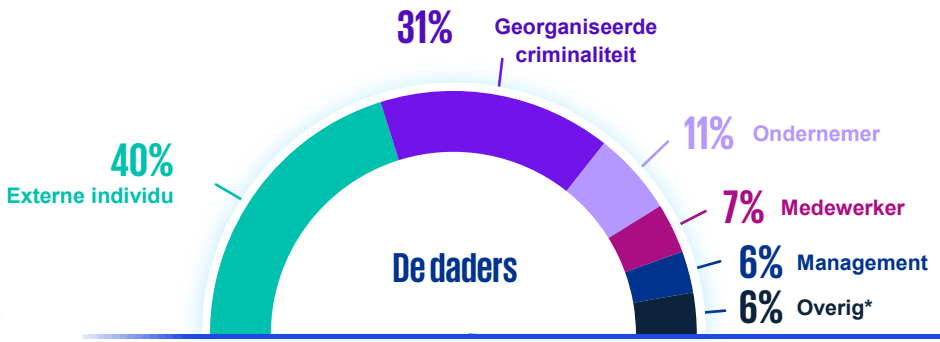
Externe individuen (9%) worden eveneens getroffen door witwasconstructies, vaak via onderliggende oplichting. Verdachte transacties moeten daarom niet alleen vanuit AML-perspectief worden beoordeeld, maar ook in samenhang met de detectie van oplichting en klantbescherming.

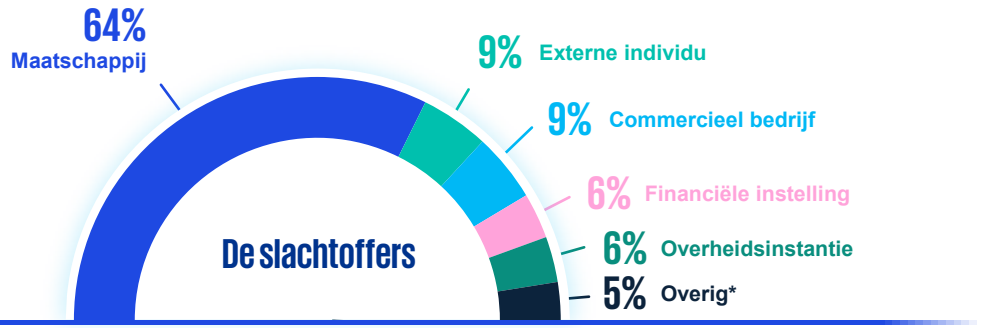
Financiële instellingen (6%) worden vooral getroffen door meer gestructureerde constructies waarin witwassen samengaat met delicten als valsheid in geschrifte, oplichting of hypotheekfraude. Deze zaken, vaak gedreven door georganiseerde criminaliteit en ondernemers, onderstrepen het belang van cliëntenonderzoek en transactiemonitoring.

Commerciële bedrijven (9%) vormen de grootste slachtoffergroep bij omkoping en corruptie. De betrokkenheid van georganiseerde criminaliteit, medewerkers en management toont hoe interne invloed kan worden misbruikt voor persoonlijk of crimineel gewin, wat een organisaties integriteit en het vertrouwen daarin kan aantasten.

Overheidsinstanties (6%) worden vooral getroffen door witwasconstructies in combinatie delicten als belastingfraude, subsidiefraude en verduistering. Het risico komt niet voort uit één daderprofiel, maar kan ontstaan door zowel intern misbruik als externe misbruik van publieke systemen of middelen.

Verdeling van daders en slachtoffers binnen het NOCLAR domein





* 'Overig' omvat de volgende typen daders: commercieel bedrijf (3,3%), klant (1,1%) en financiële instelling (1,1%).

** 'Overig' omvat de volgende typen slachtoffers: klant (4,3%), niet-commerciële instelling (0,4%) en medewerker (0,4%).

© 2026 KPMG Advisory N.V., een naamloze vennootschap en lid van het KPMG-netwerk van zelfstandige ondernemingen die verbonden zijn aan KPMG International Limited, een Engelse entiteit. Alle rechten voorbehouden.

Verdieping: 'zwendel'

Veroordelingen voor zwendel

In totaal werden 102 unieke zaken vastgesteld binnen het domein Zwendel, waaronder oplichting, computervredebreuk, cyberfraude en identiteitsfraude.

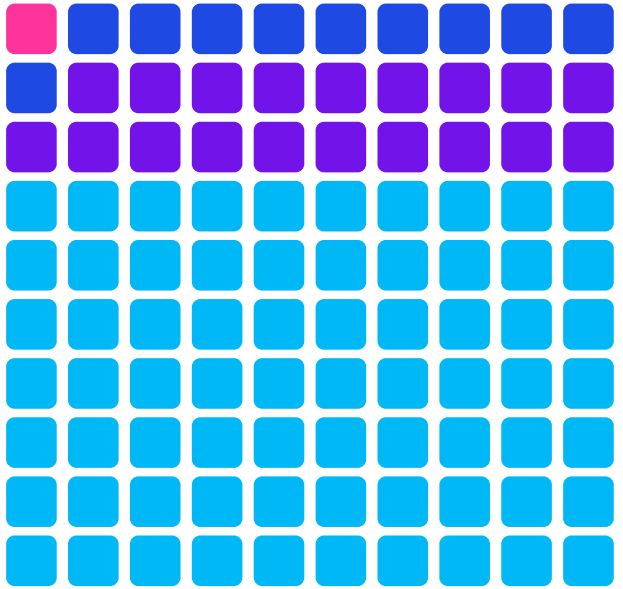
Zwendel tussen individuen komt in de praktijk voor, maar valt buiten de Fraudebarometer, die zich richt op zaken waarbij organisaties betrokken zijn. Daarom zijn alleen zaken opgenomen waarin ten minste één partij aan een organisatie verbonden is.

Oplichting vormt met 70% de duidelijke meerderheid van de veroordelingen. Bijna de helft betreft een zelfstandig delict, maar oplichting wordt ook vaak gecombineerd met valsheid in geschrifte en witwassen. Organisaties moeten dit risico daarom niet geïsoleerd beoordelen, maar als onderdeel van bredere constructies. Versterking van documentverificatie, transactiemonitoring en doorlopende beoordeling van ongebruikelijke activiteiten kan deze risico's helpen beperken.

Computervredebreuk (19%) omvat onder meer hacking, ongeautoriseerde toegang en datalekken. Deze delicten staan zelden op zichzelf en hangen vaak samen met overtredingen als cyberfraude, omkoping, schending van privacy of schending van ambtsgeheim. Misbruik van digitale toegang kan zo bredere fraude-, integriteits- en compliance-incidenten mogelijk maken. Cybermaatregelen zouden daarom moeten aansluiten op integriteits- en complianceprotocollen, in plaats van deze als afzonderlijk domein te benaderen. De sterke betrokkenheid van medewerkers maakt dit subtype bovendien relevant vanuit insider-risk perspectief. Beheersing vraagt om effectief toegangsbeheer, monitoring van afwijkende gebruikersactiviteiten en controles rond gevoelige systemen en gegevens.

Cyberfraude (10%) komt voornamelijk voor als zelfstandig delict en wordt vooral extern gedreven. Omdat cyberfraude zowel organisaties als klanten raakt, kan het bedrijfsprocessen verstoren, het vertrouwen van belanghebbenden aantasten en aanzienlijke financiële schade veroorzaken.

Verdeling van zwendel veroordelingen



- 1% Identiteitsfraude
- 10% Cyberfraude
- 19% Computervredebreuk
- 70% Oplichting

Identiteitsfraude (1%) komt uitsluitend voor in combinatie met computervredebreuk, wat laat zien hoe het kan fungeren als toegangspoort tot bredere digitale fraudeconstructies. Zelfs laagfrequente risico's kunnen hierdoor grote gevolgen hebben wanneer zij cybercriminaliteit mogelijk maken.

© 2026 KPMG Advisory N.V., een naamloze vennootschap en lid van het KPMG-netwerk van zelfstandige ondernemingen die verbonden zijn aan KPMG International Limited, een Engelse entiteit. Alle rechten voorbehouden.

De daders

Uit de analyse blijkt dat externe individuen (37%) en georganiseerde criminaliteit (16%) samen meer dan de helft van de zaken veroorzaken. Externe actoren zijn daarmee sterk vertegenwoordigd. Tegelijkertijd zijn medewerkers (17%), ondernemers (14%) en management (8%) samen goed voor bijna twee vijfde van de zaken. Dit toont aan dat zwendelrisico's zowel buiten als binnen organisaties kunnen ontstaan.

Externe individuen, **georganiseerde criminaliteit** en **ondernemers** worden vooral in verband gebracht met oplichting en cyberfraude, waarbij commerciële bedrijven, klanten en financiële instellingen vaak worden getroffen. Dit benadrukt het belang van weerbaarheid tegen externe fraudedreigingen en van integere klant- en zakelijke interacties.

Medewerkers en **management** zijn de voornaamste daders van computervredebreuk, soms in samenwerking met externe individuen. Dit toont de sleutelrol van interne toegang bij het mogelijk maken van deze delicten.

Bovendien handelde de dader in de meeste zaken niet alleen. Zwendel kan via gecoördineerde netwerken worden uitgevoerd, waarbij meerdere typen actoren samenwerken.

De slachtoffers

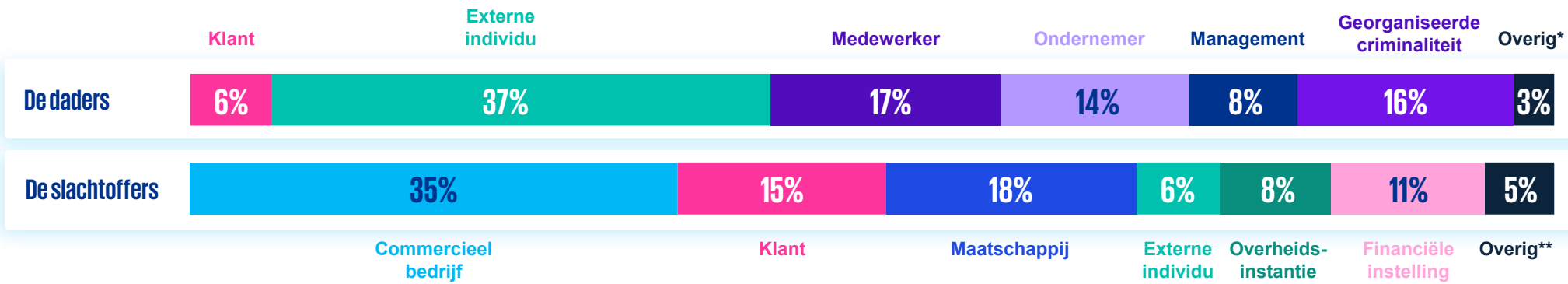
Vanuit het perspectief van slachtoffers raakt zwendel uiteenlopende belanghebbenden. **Commerciële bedrijven** vormen met 35% de vaakst getroffen groep, vooral door oplichting door externe individuen en georganiseerde criminaliteit. Ook interne risico's spelen een rol bij computervredebreuk, wanneer medewerkers toegang tot systemen, gegevens of processen misbruiken. Beheersing vraagt om een combinatie van fraude-, cyber- en interne risicomaatregelen.

Klanten (15%) worden vooral getroffen door oplichting door ondernemers. Producten, diensten en klantgerichte processen kunnen worden misbruikt om klanten te misleiden of uit te buiten.

De maatschappij (18%) is de op één na grootste slachtoffergroep, mede door de terugkerende samenhang tussen oplichting en witwassen. De impact reikt daarmee verder dan directe slachtoffers en raakt financiële integriteit en publiek vertrouwen.

Hoewel veel slachtoffers van zwendel doelbewust worden gekozen, raken **individuen** (6%) vaak als neveneffect van bredere patronen benadeeld. Zwendel kan zowel institutionele als persoonlijke schade veroorzaken. Organisaties moeten daarom verder kijken dan uitsluitend directe verliezen.

Verdeling van daders en slachtoffers binnen het Zwendel domein



* 'Overig' omvat de volgende typen daders: commercieel bedrijf (2,0%) en financiële instelling (1,0%). ** 'Overig' omvat de volgende typen slachtoffers: niet-commerciële instelling (1,9%), ondernemer (1,9%) en medewerker (1,3%).

© 2026 KPMG Advisory N.V., een naamloze vennootschap en lid van het KPMG-netwerk van zelfstandige ondernemingen die verbonden zijn aan KPMG International Limited, een Engelse entiteit. Alle rechten voorbehouden.

Verdieping: 'integriteitsschendingen'

Integriteitsschendingen

Onze dataset bevat 73 unieke zaken rond integriteitsschendingen, verdeeld over tien subtypen, zoals afpersing, wangedrag, discriminatie en belangenverstrengeling.

In tegenstelling tot andere domeinen zijn integriteitsschendingen zeer divers: geen enkel subtype domineert en de meeste zaken staan op zichzelf. Waar overlap optreedt, betreft die vrijwel uitsluitend witwassen of zwendel.

Deze spreiding wijst erop dat integriteitsrisico's doorgaans in specifieke contexten ontstaan en niet volgens één terugkerend patroon. Organisaties hebben daarom baat bij een breed, goed geïntegreerd kader dat verschillende soorten gedrag aanpakt, in plaats van beperkte beheersmaatregelen.

Afpersing (25%) komt het vaakst voor en staat meestal op zichzelf. Ook bij samenloop met andere delicten is geen vast patroon zichtbaar. Veroordeelde daders krijgen meestal een celstraf of taakstraf.

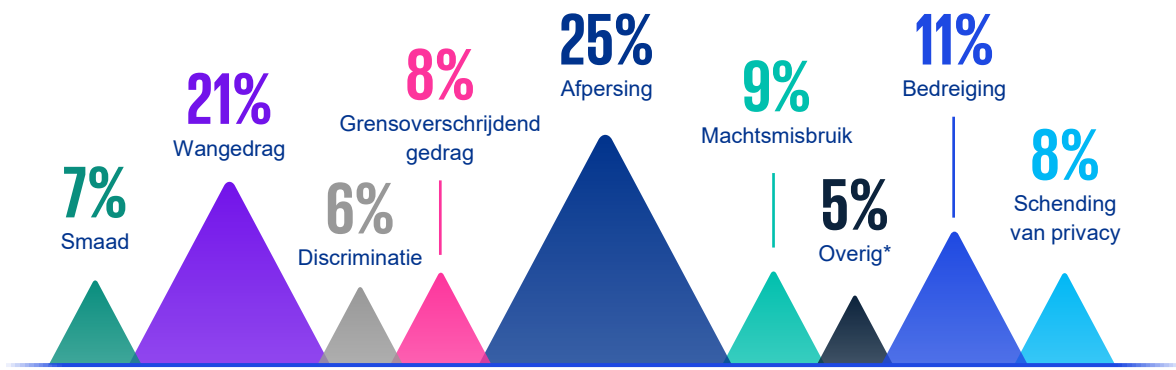
Door het onvoorspelbare karakter en de grote impact zijn afpersingsrisico's, zoals dwang of ongepaste druk, lastig te voorzien. Het onderstreept het belang van sterke interne meldkanalen en een cultuur waarin medewerkers zich veilig voelen om zich uit te spreken.

Wangedrag (21%) staat eveneens meestal op zichzelf. Rechters leggen vaak financiële of arbeidsrechtelijke gevolgen op, zoals ontslag of schorsing. Dit kan erop wijzen dat wangedrag vaak binnen bestaande werkrelaties plaatsvindt en benadrukt het cruciale belang van interne governance, disciplinaire procedures en duidelijke gedragscodes.

Bij **bedreiging** (11%) is een andere dynamiek zichtbaar: dit houdt vaker verband met andere financieel-economische criminaliteit. Door de uiteenlopende combinaties lijkt bedreigend gedrag vaak een faciliterende rol te spelen in bredere constructies. Het moet daarom niet als een op zichzelf staand probleem worden gezien, maar als mogelijk vroeg waarschuwingssignaal voor complexer wangedrag.

Over het geheel genomen zijn integriteitsschendingen divers en sterk contextafhankelijk; ze omvatten uiteenlopend gedrag binnen organisaties. Daarom zijn ze niet effectief te beheersen met geïsoleerde of reactieve maatregelen. Bedrijven hebben een proactieve, verankerde aanpak nodig die sterke governance, continue monitoring en een cultuur van transparantie en verantwoording combineert. Dit is essentieel voor vroegtijdige signalering én om escalatie naar juridische, financiële of reputatieschade te voorkomen.

Verdeling van integriteitsschendingen



* 'Overig' omvat de volgende subtypen: schending van ambtsgeheim (2,4%) en belangenverstrengeling (2,4%).

© 2026 KPMG Advisory N.V., een naamloze vennootschap en lid van het KPMG-netwerk van zelfstandige ondernemingen die verbonden zijn aan KPMG International Limited, een Engelse entiteit. Alle rechten voorbehouden.

De daders

In de 73 zaken rond integriteitsschendingen is het merendeel van de veroordelingen toe te schrijven aan drie groepen: medewerkers, externe individuen en management (samen 85%). Dit weerspiegelt zowel interne blootstelling als verschillende risicopatronen.

Medewerkers zijn betrokken bij bijna alle typen integriteitsschendingen, zonder duidelijke concentratie bij één delict. Hun handelen betreft doorgaans één type delict en maakt zelden deel uit van bredere constructies met meerdere aanklachten. Dit wijst erop dat integriteitskwesties rond medewerkers vaak voortkomen uit situationele of gedragsfactoren, niet uit structureel wangedrag. Voor organisaties onderstreept dit het belang van preventie, zoals bewustwording, training en een sterke ethische cultuur.

Externe individuen, daarentegen, laten een veel gerichter patroon zien. Hun betrokkenheid concentreert zich vooral op afpersing en bedreiging, vaak in combinatie met financieel gemotiveerde delicten zoals witwassen. Bedrijven en hun medewerkers zijn hierbij de belangrijkste doelwitten en het handelen is doorgaans bewust en doelgericht. Sterke waarborgen op cruciale contactmomenten vormen een belangrijke verdedigingslinie, vooral bij financiële transacties of externe afhankelijkheden.

Management als dader houdt vooral verband met wangedrag, machtsmisbruik en grensoverschrijdend gedrag. Deze delicten komen doorgaans voort uit misbruik van bevoegdheden, niet uit externe motieven. Ze raken niet alleen het slachtoffer, maar hebben meestal ook gevolgen voor de cultuur binnen het team en de organisatie.

De slachtoffers

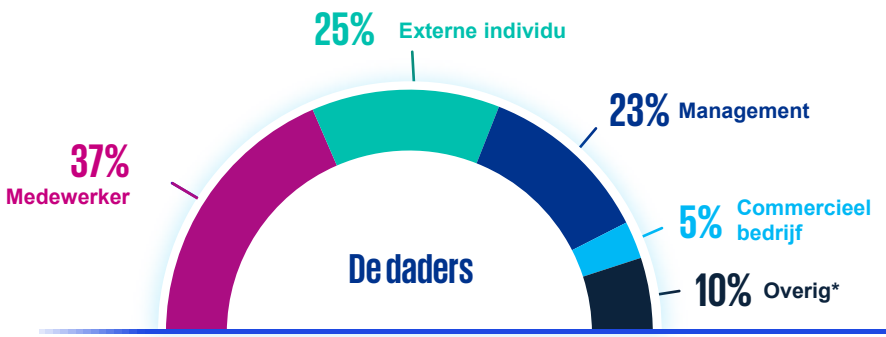
Medewerkers zijn het vaakst slachtoffer in zaken rond integriteitsschendingen, gevolgd door commerciële bedrijven. Andere partijen, zoals overheidsinstanties en niet-commerciële instellingen, worden minder vaak geraakt.

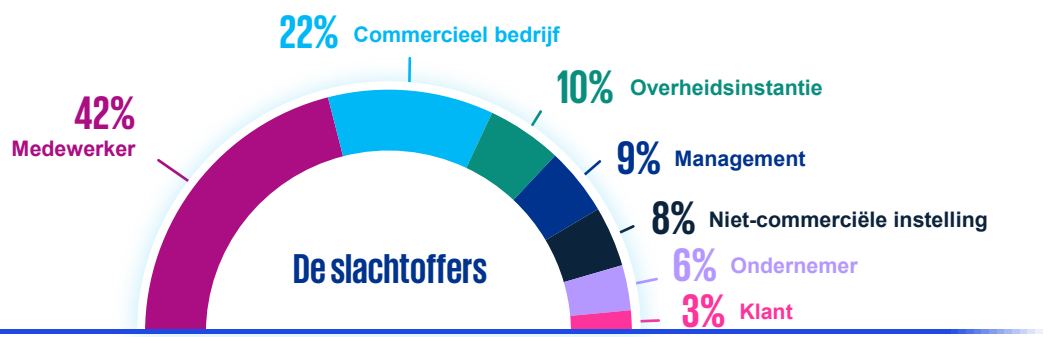
Medewerkers (42%) vormen meestal de enige slachtoffergroep en worden geconfronteerd aan een breed spectrum aan integriteitsschendingen, waaronder afpersing, machtsmisbruik en bedreiging. Dit benadrukt hun kwetsbaarheid binnen organisaties, vooral wanneer machtsongelijkheid of interpersoonlijke druk een rol speelt. Een veilige werkomgeving, ondersteund door toegankelijke meldkanalen, duidelijk beleid en betrouwbare opvolgingsprocedures, helpt organisaties deze risico's aan te pakken.

Commerciële bedrijven (22%) worden vooral geraakt door afpersing en wangedrag, meestal in de vorm van geïsoleerde, financieel gemotiveerde incidenten. Dit laat zien dat sterke interne beheersmaatregelen en duidelijke processen, met name op financieel en operationeel gebied, essentieel zijn om deze risico's te beperken.

Integriteitsrisico's ontstaan zowel intern als extern: van incidenten rond medewerkers tot externe bedreigingen en ingrijpende zaken op managementniveau. Beheersing vraagt om een evenwichtige aanpak die een sterke interne cultuur en toezicht combineert met betrouwbare externe controles. Zo kunnen organisaties problemen vroeg signaleren en de impact beperken.

Verdeling van daders en slachtoffers binnen het integriteits-schendingen domein





* 'Overig' omvat de volgende typen daders: overheidsinstantie (4,1%), klant (2,7%), ondernemer (1,4%) en niet-commerciële instelling (1,4%).

© 2026 KPMG Advisory N.V., een naamloze vennootschap en lid van het KPMG-netwerk van zelfstandige ondernemingen die verbonden zijn aan KPMG International Limited, een Engelse entiteit. Alle rechten voorbehouden.

Van inzichten naar actie

De bevindingen in deze eerste editie van de KPMG Fraudebarometer onderstrepen het brede, complexe en veranderende karakter van financieel-economische criminaliteit in Nederland. Frauderisico's beperken zich niet tot één profiel, sector of werkwijze. Ze zijn veelzijdig, betreffen zowel externe individuen als insiders en combineren vaak meerdere delicten in gestructureerde, doelbewuste constructies. De impact reikt bovendien verder dan individuele slachtoffers en raakt organisaties, instellingen en de maatschappij als geheel.

Belangrijkste inzichten

Naarmate constructies complexer worden en technologie zich verder ontwikkelt, hebben organisaties een proactieve, geïntegreerde en datagedreven aanpak nodig die preventie, detectie en respons combineert. Op basis van deze bevindingen helpen de volgende acties organisaties hun weerbaarheid tegen fraude-, integriteits- en financiële-criminaliteitsrisico's te versterken:

Medewerkers en management zijn betrokken bij uiteenlopende delicten, van verduistering en valsheid in geschrifte tot computervredebreuk. Het beheersen van intern risico vraagt meer dan traditionele controles: effectief toezicht, toegangsbeheer, functiescheiding en data-analyse helpen afwijkend gedrag te signaleren en de blootstelling aan nieuwe risico's te beperken.

Veel delicten komen voort uit gedrag binnen organisaties. Een sterke ethische cultuur, ondersteund door duidelijk beleid en governance, training, meldmechanismen, betrokken leiderschap en bewustwording onder medewerkers, blijft een belangrijke bescherming tegen wangedrag en bredere integriteitsrisico's.



Veel zaken omvatten meerdere delicten en daders. Onderzoeksmethoden die forensische expertise, geavanceerde analyses, technologie ondersteunde beoordeling van bewijsmateriaal en AI-ondersteunde analyse combineren, helpen organisaties de feiten snel en zorgvuldig vast te stellen en effectief op mogelijk wangedrag te reageren.

Complexere en gecoördineerde constructies vragen om effectieve beheersmaatregelen, risico gebaseerd cliëntenonderzoek, transactiemonitoring, geavanceerde analyses en AI-ondersteunde detectie. Samen helpen deze maatregelen afwijkende patronen te identificeren, de weerbaarheid tegen fraude en financiële criminaliteit te versterken en wangedrag, waaronder witwassen en andere complexe fraudeconstructies, tijdig te signaleren en te voorkomen.

© 2026 KPMG Advisory N.V., een naamloze vennootschap en lid van het KPMG-netwerk van zelfstandige ondernemingen die verbonden zijn aan KPMG International Limited, een Engelse entiteit. Alle rechten voorbehouden.

Hoe KPMG kan helpen

De inzichten in deze Fraudebarometer bouwen voort op KPMG Forensic's ruime ervaring met onderzoek naar fraude-, integriteits- en financiële criminaliteitsrisico's, waarbij datagedreven inzichten, geavanceerde analyses, AI-ondersteunde oplossingen en praktijkervaring worden gecombineerd.

Wij ondersteunen klanten met:

- **Feitenonderzoeken naar uiteenlopende financieel-economische delicten, zoals verduistering, wederrechtelijke toe-eigening en oplichting;**
- **Gedragsonderzoeken naar compliance- of integriteitsincidenten;**
- **Forensische technologiediensten met AI-toepassingen voor onder meer bewijsvergaring, e-discovery en forensische data-analyse;**
- **Modelvalidatie van AML- en sanctie compliance programma's en andere fraudepreventiemodellen;**
- **Cultuuronderzoeken, opstellen en toetsen van bedrijfsbeleid en gedragscodes, en diverse trainings- en communicatieprogramma's;**
- **Frauderisicobeoordelingen voor inzicht in de belangrijkste fraude- en wangedragsrisico's; en**
- **Oplossingen voor third-party risk management, zoals compliance due diligence bij M&A en distributeursreviews op contractuele verplichtingen.**

Neem contact op



Leonie Stolk
Partner, Hoofd Forensic NL

T +31 206568845
M +31 6 52488308
E stolk.leonie@kpmg.nl



Heleen Hoynck Van Papendrecht
Partner, Forensic Investigations

T +31 206567797
M +31 6 15073765
E hoynckvanpapendrecht.heleen@kpmg.nl



Muel Kaptein
Partner, Forensic I&C

T +31 206567794
M +31 6 51573611
E kaptein.muel@kpmg.nl



Patrick Özer
Partner, Forensic Technology

T +31 206568207
M +31 6 22694146
E ozer.patrick@kpmg.nl

© 2026 KPMG Advisory N.V., een naamloze vennootschap en lid van het KPMG-netwerk van zelfstandige ondernemingen die verbonden zijn aan KPMG International Limited, een Engelse entiteit. Alle rechten voorbehouden.

Bijlage

Methodologie

© 2026 KPMG Advisory N.V., een naamloze vennootschap en lid van het KPMG-netwerk van zelfstandige ondernemingen die verbonden zijn aan KPMG International Limited, een Engelse entiteit. Alle rechten voorbehouden.

Bijlage: Methodologie

Voor het identificeren van relevante casussen voor de Fraudebarometer heeft KPMG Forensic een gestructureerde, stapsgewijze werkwijze gehanteerd om consistentie en relevantie in de selectie, classificatie en analyse van zaken te waarborgen. De werkwijze bestond uit drie fases: het bepalen van de scope, het identificeren van relevante media-artikelen en het uitvoeren van een gedetailleerde review en classificatie van de zaken.

Het bepalen van de scope

KPMG Forensic heeft de scope van de Fraudebarometer bepaald op basis van onze forensische expertise en de typen misstanden die wij regelmatig in de praktijk tegenkomen. De Fraudebarometer richt zich daarom op de volgende gebieden van financiële en integriteit gerelateerde criminaliteit: financiële fraude, witwassen, verduistering, omkoping en corruptie, cybercriminaliteit, integriteitsschendingen, NOCLAR en greenwashing. Daarnaast zijn uitsluitend zaken meegenomen die in 2025 hebben geleid tot een formele rechterlijke uitspraak of schikking door een Nederlandse rechtbank. Tot slot richt de Fraudebarometer zich op zaken ten minste één partij betrokken is die verbonden is aan een organisatie, met uitzondering van witwaszaken vanwege hun relevantie voor de financiële sector.

Het identificeren van relevante media

Potentieel relevante artikelen zijn geïdentificeerd door middel van gestructureerde zoekopdrachten, gebaseerd op zorgvuldig ontwikkelde zoektermen en filters die aansluiten op de scope van de Fraudebarometer. De zoekopdrachten zijn uitgevoerd via LexisNexis, een uitgebreide onderzoeksdatabase die wereldwijde media-, juridische, regelgevende, sanctie- en bedrijfsinformatiebronnen samenbrengt. De Fraudebarometer is uitsluitend gebaseerd op Nederlandse mediabronnen en omvat een breed scala aan landelijke, regionale en lokale kranten, online nieuwsplatformen, tijdschriften en vakbladen. Deze gerichte zoekstrategie heeft geholpen om de dataset te beperken tot artikelen die waarschijnlijk binnen de scope van het onderzoek vielen, terwijl de selectie tegelijkertijd voldoende breed bleef om potentieel relevante artikelen niet voortijdig uit te sluiten.

Het classificeren van de zaken

De verzamelde artikelen zijn eerst gededupliceerd en vervolgens gereviewed aan de hand van de vooraf opgestelde inclusiecriteria met behulp van AI-gedreven reviewfunctionaliteiten en handmatige controles. Artikelen buiten de scope betroffen onder meer zaken met veroordelingen buiten Nederland of buiten het jaar 2025, evenals zaken die buiten de scope van financiële en integriteit gerelateerde criminaliteit vielen. De artikelen in scope zijn uitgesplitst naar individuele zaken, waarbij iedere veroordeelde persoon als afzonderlijke zaak is beschouwd. Elke zaak is geclassificeerd op basis van een gestandaardiseerde taxonomie die het fraudedomein, fraudetype, type dader, type slachtoffer, type sanctie en rechtbanklocatie omvat. Deze aanpak maakt vergelijking tussen zaken mogelijk, ondersteunt trendanalyses en biedt inzicht in de meest voorkomende fraude-, integriteits- en financiële criminaliteitsrisico's in Nederland.

Definities

Tijdens de ontwikkeling van de Fraudebarometer en de analyse in dit rapport zijn de volgende werkdefinities gehanteerd:

- **NOCLAR (Non-Compliance with Laws and Regulations):** overtredingen waarbij sprake is van het verhullen van illegale gelden of het niet naleven van wettelijke of professionele verplichtingen door personen of organisaties, waaronder tekortkomingen in governance, toezicht, vergunningen en verslaglegging.
- **Frauduleuze verslaglegging en verduistering:** overtredingen waarbij informatie, documenten of rapportageprocessen worden vervalst of gemanipuleerd, of waarbij financiële middelen, activa of andere bedrijfsmiddelen ongeoorloofd worden gebruikt of toegeëigend.
- **Zwendel:** overtredingen waarbij slachtoffers door misleiding, manipulatie of bedrog worden bewogen tot het verstrekken van geld, informatie, toegang of andere voordelen.
- **Integriteitsschendingen:** onethisch, ongepast, schadelijk of grensoverschrijdend gedrag dat het vertrouwen, de governance, integriteit, werkcultuur of professionele relaties ondermijnt.

© 2026 KPMG Advisory N.V., een naamloze vennootschap en lid van het KPMG-netwerk van zelfstandige ondernemingen die verbonden zijn aan KPMG International Limited, een Engelse entiteit. Alle rechten voorbehouden.

Sommige of alle hierin beschreven diensten zijn mogelijk niet toegestaan voor KPMG-auditcliënten en hun gelieerde ondernemingen of gerelateerde entiteiten.

kpmg.com/socialmedia

De in dit document vervatte informatie is van algemene aard en is niet toegespitst op de specifieke omstandigheden van een bepaalde persoon of entiteit. Wij streven ernaar juiste en tijdige informatie te verstrekken. Wij kunnen echter geen garantie geven dat dergelijke informatie op de datum waarop zij wordt ontvangen nog juist is of in de toekomst blijft. Daarom adviseren wij u op grond van deze informatie geen beslissingen te nemen behoudens op grond van advies van deskundigen na een grondig onderzoek van de desbetreffende situatie.

De naam KPMG en het logo zijn geregistreerde merken die onder licentie worden gebruikt door de zelfstandige ondernemingen die lid zijn van de wereldwijde KPMG organisatie.

© 2026 KPMG Advisory N.V., een naamloze vennootschap en lid van het KPMG-netwerk van zelfstandige ondernemingen die verbonden zijn aan KPMG International Limited, een Engelse entiteit. Alle rechten voorbehouden.

Document Classification: KPMG Public