Fraude en fraudepreventie

0. Inleiding

Volgens uiteenlopende schattingen kost fraude in allerlei varianten onze maatschappij jaarlijks een bedrag van 10 tot 30 miljard euro (dat is 4 tot 12 % van onze rijksbegroting!). De website van de Fraudehelpdesk, in 2011 opgericht om de bevolking een hoger fraudebewustzijn bij te brengen en slachtoffers van fraude de helpende hand te bieden, trok in februari 2014 haar miljoenste bezoeker. Het aantal meldingen van een poging tot oplichting is de afgelopen jaren gestegen. Hoewel hierdoor ook het fraudebewustzijn toe lijkt te nemen is er nog een wereld te winnen, niet alleen onder burgers maar ook onder bestuurders, controllers, commissarissen en toezichthouders.

De verschillende vormen van fraude zijn zeer divers en vaak creatief, de praktijkvoorbeelden bijna oneindig, en waarschijnlijk is fraude zo oud als de mensheid.

Deze position paper beoogt de lezer vertrouwd te maken met het begrip fraude en de veelheid van verschijningsvormen, bewust te maken van de mogelijke persoonlijke of zakelijke schadelijke gevolgen (verloren geld, goederen, tijd, gegevens, imago alsmede zakelijk of persoonlijk faillissement), draagt een kader aan voor preventie inclusief de rol daarin van de externe accountant en verwijst voor verdere informatie naar belangrijke externe bronnen.

De opbouw van dit document is als volgt:

Bij het schrijven van deze notitie zijn mede de volgende bronnen gebruikt:

- Nadere voorschriften controle- en overige standaarden registeraccountants
- www.dezaak.nl
- www.eversheds.nl
- www.facto.nl
- www.nctv.nl
- www.opgelicht.nl
- www.wikipedia.nl

Cees in ’t Veld/Focus op verbeteren, 1 april 2015

1. Wat is fraude?

De vroegste vindplaats van het woord fraude in het Nederlandse taalgebied is een document uit 1293 uit Brugge. Het woord is waarschijnlijk vanuit het Latijn via het Frans in de Nederlandse taal terechtgekomen; in het Latijn betekent het woord "fraus" bedrog, schade of misdaad.

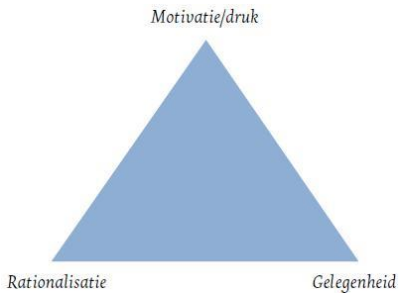
Er bestaat geen duidelijke definitie van fraude. In het Nederlandse Wetboek van Strafrecht komt de term alleen voor in artikel 273f over mensenhandel.

Fraude is een vorm van bedrog. Bedrog is eveneens een breed begrip, maar daar zijn wel duidelijker definities van. Grofweg kan worden gesteld dat sprake is van bedrog als een overeenkomst wordt aangegaan tussen twee (of meer) partijen, waarbij minimaal één van de partijen een verkeerde voorstelling van zaken heeft en dus de overeenkomst aangaat op basis van foutieve of onvolledige informatie.

Fraude is een containerbegrip. Kenmerkende elementen die aanwezig moeten zijn om van fraude te spreken zijn:

- het gaat om opzettelijk handelen;
- er wordt een misleidende voorstelling van zaken gegeven;
- er is het oogmerk economisch voordeel (financieel gewin) te behalen;
- er is een benadeelde;
- er is sprake van onrechtmatig of onwettig handelen.

Volgens controlestandaard 240 voor registeraccountants (zie verder paragraaf 4) is fraude: ‘een opzettelijke handeling door één of meer leden van het management, met governance belaste personen, werknemers of derden, waarbij gebruik wordt gemaakt van misleiding teneinde een onrechtmatig of onwettig voordeel te verkrijgen.’
Deze standaard noemt drie kenmerken (motivatie of druk, een waargenomen gelegenheid, en bepaalde argumenten ter rechtvaardiging of rationalisatie) die gezamenlijk kunnen leiden tot fraude.



Voorbeelden van fraude zijn opgenomen in bijlage 1. Een stelregel om te ontdekken of het om oplichting gaat is de volgende: "Als het te mooi is om waar te zijn, dan is het niet waar".

2. Wettelijk kader

Het Wetboek van Strafrecht kent de volgende titels die met fraude en bedrog samenhangen:

- Titel VIII. Misdrijven tegen het openbaar gezag (waaronder omkoping ambtenaren)
- Titel XI. Valsheid in zegels en merken
- Titel XII. Valsheid met geschriften, gegevens en biometrische kenmerken
- Titel XVII. Schending van geheimen
- Titel XXII. Diefstal en stroperij
- Titel XXIII. Afpersing en afdreiging
- Titel XXIV. Verduistering
- Titel XXV. Bedrog
- Titel XXVI. Benadeling van schuldeisers of rechthebbenden
- Titel XXX. Begunstiging (heling)
- Titel XXXA. Witwassen

Voorts kunnen de Amerikaanse Foreign Corrupt Practices Act (FCPA) en met name de Britse United Kingdom Bribery Act (Bribery Act) wegens hun extraterritoriale werking rechtstreeks van toepassing zijn op Nederlandse personen of ondernemingen.

Kort gezegd valt een persoon of onderneming die handelt namens een Amerikaanse onderneming of een dochter daarvan, onder de werking van de FCPA. Daarnaast vallen gedragingen onder de FCPA indien gebruik is gemaakt van interstatelijk handelsverkeer, hetgeen niet meer behoeft in te houden dan een internetbetaling van of naar een Amerikaanse bank, of e-mailverkeer in en naar de Verenigde Staten.

De Bribery Act bepaalt dat niet alleen gedragingen die plaatsvinden op het territorium van het Verenigd Koninkrijk onder de Bribery Act vallen, maar ook gedragingen daarbuiten door een (rechts)persoon met een ‘close connection’ met het Verenigd Koninkrijk (bijvoorbeeld Britse onderdanen, of entiteiten opgericht naar Engels recht en mogelijk hun dochtervennootschappen, agenten en dienstverleners). Ook indien de handelingen (waar ook ter wereld) gepleegd worden door een persoon of onderneming (of diens dochter, agent of werknemer) die zaken doet of heeft gedaan met het Verenigd Koninkrijk (zoals een vestiging of distributienetwerk), is de Bribery Act van toepassing. Kortom, deze buitenlandse wetgeving heeft een dusdanig ruim toepassingsbereik dat ook in Nederland woonachtige of gevestigde (rechts)personen met de gevolgen in aanraking kunnen komen.

Zowel de Bribery Act als de FCPA kennen hoge straffen (ongelimiteerde) boetes en gevangenisstraffen), die kunnen worden opgelegd aan zowel de onderneming als aan individuele bestuurders en andere personen betrokken bij de gesanctioneerde handelingen. Veroordelingen kunnen openbaar gemaakt worden met reputatieschade als gevolg. De Bribery Act kent bovendien de sanctie van uitsluiting voor aanbestedingen voor de betreffende onderneming, iets dat met name ondernemingen actief in bouw en ontwikkeling hard kan raken.

3. Preventie van fraude

Gezien de vele verschijningsvormen van fraude is het onmogelijk om alle mogelijke preventiemaatregelen voor alle mogelijke soorten fraude in detail weer te geven. Wel wordt een algemeen kader geschetst waarbinnen effectieve preventie van fraude zijn plaats kan krijgen.

3.1 Leiderschap, gedrag en organisatie

Het management, onder toezicht van de met governance belaste personen, houdt een cultuur van eerlijk en ethisch gedrag in stand en vervult een voorbeeldfunctie in het uitdragen van deze cultuur en het aanspreken van personen die ongewenst gedrag vertonen (‘tone at the top’).

Gewenst gedrag is expliciet gemaakt via zaken als een gedragscode (bij voorkeur ingericht via principes), reglementen die zijn gekoppeld aan de arbeidsovereenkomst (waaronder algemene regels, gebruik van goederen, gebruik van internet, omgang met gegevens), het aanstellen van vertrouwenspersonen en het instellen van een klokkenluidersregeling.

Alertheid op fraude zou onderdeel van de cultuur moeten zijn, ondersteund door een adequate procedure voor het melden van (verdenking van) fraude en een draaiboek bij het ontdekken van fraude.

3.2 Strategie en risicomanagement

De organisatie kent een gestructureerd proces van risicomanagement (waaronder frauderisico’s), onder meer inhoudende:

- het identificeren van bedrijfsrisico’s die het realiseren van de doelstellingen van de organisatie zouden kunnen bedreigen;
- het inschatten van de significantie van deze risico’s;
- het inschatten van de waarschijnlijkheid dat deze risico’s zich voordoen;
- het nemen van beslissingen over te ondernemen acties op om deze risico’s in te spelen.

3.3 Inrichting van processen

De organisatie onderhoudt een adequate interne beheersing van haar processen om in te spelen op geïdentificeerde bedrijfsrisico’s (waaronder frauderisico’s) die een bedreiging vormen voor het realiseren van de doelstellingen van de organisatie, die betrekking hebben op:

- de effectiviteit en efficiency van haar activiteiten;
- de betrouwbaarheid van de financiële verslaglegging van de organisatie;
- de naleving van wet- en regelgeving door de organisatie.

De wijze waarop de interne beheersing is ingericht is mede afhankelijk van de omvang en de complexiteit van de organisatie.

Belangrijke maatregelen van interne beheersing zijn:

- het instellen van gedragscode en reglementen;
- het instellen van procedures;
- screening van personeel, leveranciers en afnemers;
- het (al dan niet gezamenlijk) verlenen van bevoegdheden aan bepaalde personen, met een escalatie bij grotere belangen en/of risico's;
- offerteprocedures voor inkopen;
- periodiek toetsen van inkoopprijzen en -voorwaarden in de markt;
- autorisatie van verkoopprijzen en kortingstabellen;
- functiescheiding;
- vier ogen principe;
- fysieke beveiliging;
- logische toegangsbeveiliging;
- 'çlean desk';
- oogtoezicht;
- toezicht via camera's;
- fouillering bij vertrek na werktijd (al dan niet steekproefsgewijs);
- gescheiden bewaring;
- periodieke inventarisatie;
- registratie van de bedrijfsactiviteiten;
- registratie van afval/uitval/derving/voorraadverschillen/verschrotting
- analyse van informatie.

Zie ook Bijlage 2 Checklist fraudepreventie.

3.4 Beheer van middelen

3.4.1 Kasgeld

Kasgeld is zeer diefstalgevoelig en dient daarom fysiek goed beveiligd te zijn in een afgesloten kas die achter slot en grendel (zo mogelijk een kluis) wordt bewaard.
Bij voorkeur is een specifiek aangewezen persoon verantwoordelijk voor het kassaldo.
Periodieke inventarisatie en adequaat sleutelbeheer zijn essentieel.

3.4.2 Banktegoeden

Banktegoeden zijn bijna gelijk te stellen aan kasgeld, hoewel onrechtmatige overboeking van gelden meestal wel sporen nalaat. Het beperken van het aantal specifieke personen aan wie bevoegdheden tot betaling zijn toegekend (met eventueel gezamenlijke bevoegdheid voor grotere bedragen) alsmede functiescheiding (voorbereiding betalingen, goedkeuring betalingen, registratie geldverkeer) en maximering van betalingslimieten bij telebankieren zijn van groot belang.
Een bekend risico is de gouden greep: in één keer een groot bedrag naar jezelf overmaken en doorsluizen en maken dat je wegkomt.

3.4.3 Goederen

Goederen (in de vorm van machines, installaties, computers, auto's, voorraden) zijn diefstalgevoeliger naarmate ze waardevoller zijn. Fysieke beveiliging, beheer door daartoe aangewezen personen, oogtoezicht, cameratoezicht, (steekproefsgewijze) fouillering bij vertrek na werktijd, regels voor gebruik door medewerkers, periodieke inventarisatie en een adequate vernietigingsprocedure zijn van groot belang. Wees alert op activa die op projecten zijn weggeschreven en dus niet meer in de administratie geregistreerd zijn.

3.4.4 Tijd

De hoofdregel is dat de aan de medewerker (via het salaris) betaalde uren inclusief overuren (shoptime) worden besteed aan direct produktieve uren (jobtime), indirect produktieve uren (vergaderen, offertes e.d.) en niet beïnvloedbare uren (feestdagen, vakantie, ziekte e.d.), waarbij de indirecte uren op jaarbasis zijn genormeerd.

Analyse van de aansluiting jobtime-shoptime voor direct personeel dient periodiek (per dag/week/maand/kwartaal) plaats te vinden. De beoordeling of uren weglekken is voor indirect personeel moeilijker te maken dan voor direct personeel. Beoordeling van de output van de medewerker en oogtoezicht kunnen hierin een rol spelen.

3.4.5 Gegevens

Het probleem met gegevens is dat ze digitaal of fysiek kunnen worden gekopieerd zonder dat dit wordt gesignaleerd: je bent ogenschijnlijk niets kwijt. Het feit dat kopiëren niet altijd sporen nalaat stelt daarom hoge eisen aan de beveiliging van gegevens.
Fysieke beveiliging van belangrijke hardcopy gegevens, adequate 'back up en recovery' procedures, een duidelijke en nageleefde 'çlean desk' procedure en adequate procedures op het gebied van ICT (zie 3.5 hierna) zijn van groot belang.

3.5. ICT

Bijna elke organisatie werkt tegenwoordig digitaal, met computers op kantoor, op laptops en smartphones die ook buiten kantoor gebruikt kunnen worden en steeds vaker via het internet (de 'cloud') waar ook gegevens worden opgeslagen. Daarnaast hebben veel bedrijven een website waarmee ze in contact staan met klanten. Op veel websites kunnen klanten ook hun bestelling doen.
Digitaal verzamelt een bedrijf dus veel: klantgegevens, financiële informatie, bedrijfskritische documenten zoals prijslijsten, personeelsdossiers enz. En steeds vaker gaan processen in het bedrijf ook digitaal: betalingen, bestellingen van klanten en bij de toeleverancier en het aansturen van productie.
Zoals bedrijfsbelangen, gelden en goederen fysiek worden beschermd moet ook de digitale informatie van een organisatie continu worden beschermd tegen onder andere hackers, virussen en gegevensdiefstal. Bijzondere aandacht is nodig voor de zogenaamde 'superuser'.

Belangrijke maatregelen van interne beheersing van ICT zijn:

- training van en bewustwording bij medewerkers;
- fysieke beveiliging van hardware;
- scheiden van ontwikkel- en produktie-omgeving van software;
- het bewaren van broncodes van software in escrow;
- documentatie van software;
- logische toegangsbeveiliging via autorisatietabellen in combinatie met wachtwoordprocedures;
- netwerkbeveiliging;
- antiviruscontrole;
- anti spam bewaking/firewalls;
- spyware en malware controle;
- logging;
- geprogrammeerde controles;
- probleem- en incidentmanagement;
- back up, herstel en uitwijkmaatregelen;
- voorschriften voor computer- en internetgebruik.

ICT is voor bijna elke organisatie een bedrijfskritisch proces maar daarnaast ook een buitengewoon ingewikkeld vakgebied. Hierdoor is het steeds ondoenlijker om de benodigde kennis en vaardigheden in huis te hebben om zelf de beveiliging van computers en netwerk in continuïteit te garanderen. Ondersteuning van een betrouwbare ICT partner is daarom ernstig te overwegen. Ook de controlerend accountant kan hierin een belangrijke rol worden gegeven.

3.6 Interne controle

De meeste van de hiervoor genoemde maatregelen hebben een preventief karakter. Toch kan er altijd iets mis gaan. Daarom is het van belang om op grond van een periodiek geactualiseerde risicoanalyse en een daarop gebaseerde afweging van kosten en baten een betrouwbaar stelsel van interne controle in te richten waarmee het optreden van risico's, dus ook van frauderisico's, aan de hand van kritische sturingsindicatoren worden gemonitord, geregistreerd en gerapporteerd. Omdat omstandigheden zich voortdurend kunnen wijzigen moet het stelsel van interne controle permanent up-to-date worden gehouden.

3.7 Draaiboek bij ontdekking van fraude

Indien fraude wordt gesignaleerd zijn een procedure voor het melden van fraude en een draaiboek voor het afhandelen van gesignaleerde fraude gewenst. Zie ook bijlage 3 Negen tips bij interne fraude.

4 Fraude en accountantscontrole

4.1 Algemeen

Eén van de kernactiviteiten van registeraccountants is de controle van financiële overzichten waaronder jaarrekeningen. De hierop betrekking hebbende regelgeving is onder meer vastgelegd in de Nadere voorschriften controle- en overige standaarden (NVCOS) ex artikel 24 van de Verordening gedrags- en beroepsregels accountants.

In de NVCOS zijn onder meer standaard 240 ‘De verantwoordelijk van de accountant met betrekking tot fraude in het kader van de controle van financiële overzichten’ en Standaard 250 ‘Het in aanmerking nemen van wet- en regelgeving bij een controle van financiële overzichten’ opgenomen. Hoewel Standaard 250 ook verband kan houden met fraude beperken wij ons in deze notitie tot Standaard 240, die is bedoeld als hulpmiddel voor de accountant bij het identificeren en inschatten van de risico’s op een afwijkend materieel belang die het gevolg is van fraude en bij het opzetten van werkzaamheden om dergelijke afwijkingen te detecteren.

De accountant is verantwoordelijk voor het verkrijgen van een redelijke mate van zekerheid dat de financiële overzichten als geheel geen afwijkingen van materieel belang bevatten die het gevolg zijn van fraude of fouten.

Een post in een financieel overzicht is van materieel belang indien van afwijkingen, met inbegrip van weglatingen, afzonderlijk of gezamenlijk, redelijkerwijs kan worden verwacht dat zij een invloed zullen hebben op de economische beslissingen die gebruikers op basis van de financiële overzichten nemen.

Het risico dat een afwijking van materieel belang die het gevolg is van fraude niet wordt gedetecteerd is groter dan het risico dat een afwijking van materieel belang als gevolg van fouten niet wordt gedetecteerd. Dit komt omdat fraude gepaard kan gaan met geraffineerde en zorgvuldig opgezette plannen om de fraude te verhullen, zoals valsheid in geschrifte, het opzettelijk nalaten transacties vast te leggen of het opzettelijk aan de accountant verkeerd voorstellen van zaken.

De mogelijkheid dat de accountant fraude detecteert hangt af van factoren als de vaardigheid van de dader, de frequentie en omvang van de manipulaties, de mate van samenspanning waarmee de fraude gepaard gaat, de relatieve omvang van de individuele bedragen waarmee is gemanipuleerd en de senioriteit van de bij de fraude betrokken personen. Voorts is het risico van niet ontdekking van fraude groter bij managementfraude dan bij personeelsfraude.

4.2 Doelstellingen van de accountant

De doelstellingen van de accountant zijn:

1. het identificeren en inschatten van risico's op een afwijking van materieel belang die het gevolg is van fraude;
2. het verkrijgen van voldoende en geschikte controle-informatie over de ingeschatte risico's op een afwijking van materieel belang die het gevolg is van fraude door middel van het opzetten en implementeren van geschikte manieren om op die risico's in te spelen; en
3. het op passende wijze inspelen op fraude of vermoede fraude die tijdens de controle is geïdentificeerd.

4.3 Vereisten

De accountant dient aan de volgende vereisten te voldoen:

1. De accountant dient gedurende het gehele controleproces een professioneel kritische houding aan te nemen.
2. Voorafgaand aan de controle dient de accountant met alle leden van het controleteam een bespreking te houden waarbij specifiek aandacht moet worden besteed aan de risico's van frauderisico en de wijze waarop deze gepleegd zouden kunnen worden. Hierbij moet worden voorbijgegaan aan het beeld dat management en de met governance belaste personen eerlijk en integer zijn.
3. Bij de uitvoering van risico-inschattingswerkzaamheden gericht op het verwerven van inzicht in de organisatie en de interne beheersing besteedt de accountant verplicht aandacht aan:
    - het management en anderen binnen de organisatie;
    - de met governance belaste personen;
    - geïdentificeerde of ongebruikelijke of onverwachte verbanden;
    - overige informatie;
    - het evalueren van frauderisicofactoren.

Na stap 2 en 3 volgen de uitvoering van de controle, de evaluatie van de controlebevindingen en de rapportage, ook ten aanzien van fraude. Al deze stappen dienen adequaat in het controledossier te worden gedocumenteerd.

Uit het voorgaande blijkt dat de controlerend accountant jaarlijks verplicht nadenkt over de concrete frauderisico's binnen de te controleren organisatie en dat hij/zij de resultaten van dit proces ook vastlegt in het controledossier.
Helaas is de realiteit dat de uitkomsten van dit proces lang niet altijd of slechts summier met het management worden gedeeld, waardoor het management relevante informatie wordt onthouden. Het is daarom verstandig om als management met de controlerend accountant zelf de dialoog te zoeken over frauderisico's.

5. Bronnen voor verdere informatie

Verdere relevante informatie inzake fraude is onder meer te vinden op de websites van:

- Fraudehelpdesk;
- Opgelicht?!;
- Nationaal Cyber Security Centrum;
- Bescherm je bedrijf;
- Veilig internetten;
- De Zaak;
- Facto;
- Hoffman Bedrijfsrecherche.

5.1 Fraudehelpdesk

De Fraudehelpdesk (www.fraudehelpdesk.nl) wil zoveel mogelijk voorkomen dat de Nederlandse bevolking slachtoffer wordt van fraude. Hun doel is burgers en bedrijven te behoeden voor oplichtingspraktijken en weerbaarder te maken tegen fraude door mensen bewust te maken van de risico's op fraude. Zo wordt voor frauduleuze zaken gewaarschuwd op de website, Facebook en Twitter.

De Fraudehelpdesk is er voor al uw vragen en meldingen over fraude. Fraudeslachtoffers wordt de helpende hand geboden door hen naar de juiste instantie te verwijzen, zodat de gedupeerde niet zelf op zoek hoeft naar het goede adres voor hulp.

De Fraudehelpdesk heeft geen opsporingsbevoegdheid en maakt met zijn activiteiten en dienstverlening deel uit van Stichting Aanpak Financieel-Economische Criminaliteit in Nederland (SafeCin).

5.2 Opgelicht?!

Op deze website van AvroTros (www.opgelicht.nl) staan uitzendingen, alerts, nieuws, hulp en een scala van dossiers met oplichtingsmethoden in de rubrieken Bedrijven en producten, Financieel en juridisch, Gezondheid, Internet, Kansspelen, Nigeriaanse fraude, Personen, Telefonie, Vakantie en vrije tijd, Vervoer, Wonen en vastgoed en Overig.

5.3 Nationaal Cyber Security Centrum

De opkomst van moderne informatie- en communicatietechnologie (ICT) heeft de samenleving ingrijpend gewijzigd. Naast de fysieke samenleving is een digitale samenleving ontstaan, waarin we onze bankzaken regelen, inkopen doen en elkaar op tal van platforms tegenkomen. De toenemende afhankelijkheid van ICT maakt niet alleen de samenleving en de economie, maar ook organisaties kwetsbaar. Een samenleving zonder internet is nog nauwelijks denkbaar. Om de samenleving en de economie niet te verstoren is digitale veiligheid, of cyber security, van vitaal belang. Cyber security is het vrij zijn van gevaar of schade veroorzaakt door verstoring of uitval van ICT of door misbruik van ICT.
Het gevaar of de schade door misbruik, verstoring of uitval kan bestaan uit beperking van de beschikbaarheid en betrouwbaarheid van de ICT, schending van de vertrouwelijkheid van in ICT opgeslagen informatie of schade aan de integriteit van die informatie.

Om die reden heeft de overheid besloten tot het ontwikkelen van een Nationale Cyber Security Strategie (NCSS). Onderdeel van deze strategie is de oprichting van een Nationaal Cyber Security Centrum (www.ncsc.nl). per 1 januari 2012. Het NCSC bestaat uit een samenwerking van publieke en private organisaties die zich richt op een integrale aanpak van cyber security. Binnen het NCSC wordt tactische en operationele kennis en expertise uit de publieke en private sectoren bij elkaar gebracht. Op deze manier komt er meer inzicht in ontwikkelingen, dreigingen en trends en kan er meer ondersteuning worden gegeven bij incidentafhandeling en crisisbesluitvorming op het gebied van digitale veiligheid.

5.4 Bescherm je bedrijf

De website www.beschermjebedrijf.nl heeft tot doel MKB-bedrijven bewuster te maken van informatiebeveiliging en bedrijven praktische stappen te geven hoe u met informatiebeveiliging in uw eigen organisatie aan de slag kunt gaan. Deze website is een initiatief van Nederland ICT, de branchevereniging voor ICT- en telecombedrijven in Nederland.

5.5 Veilig internetten

Veilig internetten (www.veiliginternetten.nl) is een website waar u tips, trucs en praktische stap voor stap uitleg kunt vinden over wat u kunt doen en laten om veilig te internetten. Deze site is bedoeld voor iedereen met vragen over veilig gebruik van internet.Veiliginternetten.nl is een gezamenlijk initiatief van het ministerie van Economische Zaken, het ministerie van Veiligheid en Justitie / Nationaal Cybersecurity Centrum, ECP | Platform voor de Informatiesamenleving en het bedrijfsleven en is geen helpdesk. Bij diverse onderwerpen staat vermeld bij wie u terecht kunt voor individueel advies en ondersteuning.

5.6 De Zaak

De Zaak (www.dezaak.nl) is een kennisnetwerk voor ondernemers in het midden- en kleinbedrijf. Na het intypen van het zoekwoord ‘fraude’ verschijnt een serie nuttige artikelen over fraude.

5.7 Facto

Facto online www.facto.nl is het online platform voor de facility professional. Na het intypen van het zoekwoord ‘fraude’ verschijnt een serie nuttige artikelen over fraude.

5.8 Hoffman Bedrijfsrecherche

Hoffman Bedrijfsrecherche (www.hoffmannbv.nl) is sinds 1962 zelfbenoemd marktleider op het gebied van bedrijfsrecherche en fraudepreventie. Hoffmann helpt u om uw organisatie te beschermen tegen fraude van binnenuit of van buitenaf, zoals onterecht ziekteverzuim, interne diefstal en oneigenlijk internetgebruik. Hun filosofie daarbij is dat uw medewerkers zowel de zwakste als de sterkste schakel in uw beveiliging tegen fraude zijn. Hoffmann heeft drie afdelingen: Bedrijfsrecherche, ICT-Security en Consultancy & Opleidingen.

Bijlage 1 Voorbeelden van fraude

Acquisitiefraude: mensen of bedrijven worden overgehaald een advertentie te plaatsen tegen een hoog bedrag, terwijl de advertentie later niet geplaatst zal worden.

Belastingfraude (ook wel: belastingontduiking): minder of geen belasting betalen door het niet naleven van de fiscale wetgeving. Bij belastingontduiking is er altijd sprake van een wetsovertreding.

Bouwfraude: afspraken die in strijd zijn met mededingingsregels worden verzwegen.

BTW-fraude: de inning van btw wordt gedwarsboomd door een zgn. btw-carrousel op te zetten van lege BV's die elkaar leveringen doen (eventueel fictief of altijd dezelfde goederen) waarbij BTW niet afgedragen wordt en voorbelasting onterecht teruggevorderd. Het verschil met 'normale' belastingfraude is dat de overheid niet zozeer geld misloopt maar zelfs rechtstreeks geld afhandig wordt gemaakt (dit lijkt op subsidiefraude).

Copyfraude: er worden auteursrechten geclaimd, terwijl diegene niet de juridische controle heeft over een werk.

Datafraude (gegevensfraude): hierbij wordt onrechtmatig voordeel behaald via de diefstal of het gebruik van gegevens of groepen van gegevens.

Declaratiefraude: het ten onrechte of bovenmatig declareren van kosten.

Diplomafraude: hierbij wordt beweerd dat men een titel of diploma heeft terwijl dit niet zo is, of wordt een vals diploma gebruikt. Hieraan verwant is **C.V.-fraude**: het vermelden van onwaarheden op het C.V.. Dit alles geschiedt om de eigen onderneming of positie op de arbeidsmarkt te verbeteren.

Directiefraude (managementfraude): fraude waarbij één of meer directieleden of leden van de organen belast met governance zijn betrokken.

Dopingfraude: het gebruiken van niet toegestane stimulerende middelen in de sport.

Examenfraude: hierbij spiekt de leerling of student, waardoor zijn leraren geen juist beeld van zijn kennis krijgen.

Factuurfraude: het onrechtmatig verkrijgen van voordeel door te hoge inkoopfacturen of te lage verkoopfacturen.

Faillissementsfraude: hierbij worden geld of middelen vlak voor het faillissement uit de onderneming vervreemd, waardoor schuldeisers geen beslag kunnen leggen op de bezittingen.

Hacken: (het ongeoorloofd binnendringen op iemands computer).

Huurfraude: hierbij wordt een pand gehuurd maar wordt er geen huur betaald, waarbij de uitzetting door vertragingstechnieken en misbruik van huurdersbescherming zoveel mogelijk wordt getraineerd.

Hypotheekfraude: een vorm van kredietfraude waarbij het onderpand een vastgoedobject is.

Identiteitsfraude: het gebruik zonder toestemming van persoonsgegevens voor financieel gewin.

Inkoopfraude: het ontvangen van steekpenningen (geld of goederen) in ruil voor het verstrekken van de opdracht of informatie in het offertetraject, het goedkeuren van facturen voor goederen of diensten die niet (volledig) zijn geleverd of het goedkeuren van facturen waarop de prijs hoger is dan de afgesproken prij dan wel het goedkeuren van vervalste facturen voor privé geleverde goederen/ diensten.

Internetfraude: hierbij vindt fraude met verschillende fraudetechnieken via het internet plaats.

Jaarrekeningfraude: hierbij wordt in de jaarrekening een onjuist beeld gegeven van de stand van zaken in een organisatie.

Koop- en verkoopfraude: het online (ver)kopen van goederen of diensten zonder die te leveren of te betalen.

Kredietfraude: hierbij wordt onder valse voorwendselen een lening of 'krediet' aangevraagd of verkregen. Wanneer het krediet niet meer kan worden afgelost blijkt het onderpand vaak minder waard te zijn dan eerder werd verondersteld. Het is goed mogelijk dat het al vanaf het begin de bedoeling was het krediet niet terug te betalen.

Loterijfraude is een vorm van voorschotfraude (zie hierna). De ‘winnaar’ krijgt een telefoontje, mail of sms met de boodschap dat hij/zij een groot geldbedrag heeft gewonnen in een loterij. De ‘winnaar’ moet contact opnemen met de organisatie om de prijs in ontvangst te nemen. Om het verhaal geloofwaardig te maken, tonen de oplichters vaak authentiek lijkende certificaten en documenten. Degene die reageert, krijgt al snel de vraag een bedrag over te maken voor “kosten die noodzakelijk zijn om het geld te ontvangen”.
In het begin gaat het vaak om kleine bedragen. Daarna worden de kosten steeds hoger.
Het bedrag dat de ‘winnaar’ betaalt, kan als verloren worden beschouwd. Ook de beloofde geldprijs wordt niet uitgekeerd. Ook vragen de fraudeurs onder meer om persoonlijke informatie of kopieën van officiële documenten, zoals uw paspoort of rijbewijs. Deze gegevens zijn nodig om uw identiteit te bevestigen staat in het bericht, maar de fraudeurs kunnen deze informatie gebruiken om identiteitsfraude (zie hiervoor) te plegen. Deze fraude wordt meestal door Nigerianen toegepast. Daarom wordt het ook wel 419-fraude genoemd, naar artikel 4.19 van het Nigeriaanse strafrecht.

Pishing: het ‘vissen’ naar vertrouwelijke informatie met behulp van internet of e-mail. Het doel van een ‘phishe’ is om gegevens te misbruiken om bijvoorbeeld geld over te boeken of goederen aan te schaffen. Het is dus een digitale manier van iemand oplichten. Een ‘pisher’ doet zich meestal voor als een gerenommeerde organisatie, bijvoorbeeld een bank of online winkel.

Salarisfraude: het uitbetalen van een te hoog salaris of te hoge kostenvergoedingen.

Subsidiefraude: hierbij wordt onder valse voorwendselen ten onrechte subsidie aangevraagd.

Systeemfraude: de Nederlandse overheid hieronder iedere poging tot het laten uitbetalen door de belastingdienst van een bedrag dat is gebaseerd op onjuiste gegevens, bijvoorbeeld door voorlopige teruggaven van loon- of omzetbelasting, of voorlopige uitbetaling van toeslagen. Systeemfraude kan gepaard gaan met identiteitsfraude (zie hiervoor). Ook kan het initiatief uitgaan van een bemiddelaar, en gebeuren op naam van een betrokkene die meedeelt in de buit, en/of meewerkt zonder te begrijpen wat hij ondertekent. In hoeverre degene op wiens naam de fraude plaatsvindt dader is en in hoeverre slachtoffer kan dus variëren.

Uitkeringsfraude: personen die onder valse voorwendselen ten onrechte een (te hoge) uitkering genieten;

Verkiezingsfraude: hierbij wordt geknoeid met verkiezingsuitslagen, waardoor de kiezers en het buitenland een onjuist beeld krijgen van de verkiezingen, en een politicus ten onrechte wordt geïnstalleerd.

Werknemersfraude (personeelsfraude): fraude waarbij uitsluitend personeelsleden van een organisatie zijn betrokken.

Verzekeringsfraude: hierbij tracht een verzekerde een verzekeringsmaatschappij onder valse voorwendsels tot uitkering te doen overgaan of een verzekering onder valse voorwendsels aan te vragen.

Voedselfraude: hierbij wordt een bepaald etenswaar vervangen door een ander, vaak goedkoper etenswaar zonder dat de eter weet dat dit product is verwisseld. Het is mogelijk dat consumptie van dit etenswaar gevaar voor de gezondheid oplevert (bedorven vlees, verontreinigde alcohol etc.).

Voorschotfraude (beter bekend als 'Nigeriaanse oplichting'): hierbij wordt gevraagd om een rekening ter beschikking te stellen waarop een enorm bedrag (miljoenen USD of EUR) afkomstig van één of andere erfenis kan geparkeerd worden. Het slachtoffer wordt een deel van deze erfenis beloofd maar moet eerst allerlei verplichtingen (met kosten) vervullen. Uiteindelijk na het betalen van kosten blijkt dan dat het geld toch niet kan worden overgemaakt. Zolang het slachtoffer geen wantrouwen toont blijven de oplichters geld vragen. Deze vorm van oplichting is zeer oud en bekend maar toch lopen er nog steeds personen in de val. De technische term voor dit soort oplichtingen is ‘advance fee fraud’.

Wetenschapsfraude: hierbij worden onderzoeksresultaten verkregen door deze te baseren op gemanipuleerde, verzonnen of door plagiaat verkregen gegevens.

Witwassen: hierbij wordt de illegale herkomst van gelden verborgen via een carrousel van transacties, waardoor de gelden ogenschijnlijk legaal verkregen lijken te zijn.

Op internet zijn via de zoekterm ‘beroemde fraudezaken’ talloze beroemde fraudezaken te vinden.

Bijlage 2 Checklist fraudepreventie

Risicomanagement

- Vindt een regelmatige risicoanalyse plaats met betrekking tot criminaliteitsvormen die intern in uw onderneming kunnen voorkomen?
- Wordt hierbij rekening gehouden met de bekend geworden schadehistorie (eerdere incidenten)?
- Is aan de hand van deze risicoanalyse vastgesteld, welke onderdelen, afdelingen of locaties binnen het bedrijf een verhoogd risico lopen?
- Zijn de vertrouwensfuncties (functies met een verhoogd criminaliteits- of frauderisico) binnen de organisatie geïnventariseerd?
- Zijn met betrekking tot die afdelingen en die functies security-richtlijnen vastgesteld?
- Zijn die richtlijnen gecommuniceerd met het lijn- en personeelsmanagement en het personeel?
- Bestaat voor de risico's die binnen uw organisatie zijn geïdentificeerd, een schadefinancieringsplan?
- Zijn de risico's van intern gepleegde criminaliteit specifiek gedekt?
- Is er een fraudebeleidsplan samengesteld?
- Is dit fraudebeleidsplan gecommuniceerd met het vertegenwoordigend overleg in uw organisatie?
- Is binnen de organisatie een aangiftebeleid geformuleerd?
- Is er binnen de organisatie een sanctiebeleid ten aanzien van interne criminaliteit, onrechtmatig handelen of overtreding van de interne regelgeving?
- Zijn aangifte- en sanctiebeleid met het personeel gecommuniceerd?
- Bestaat er een duidelijke scheiding tussen de uitvoerende en de controlerende taken binnen uw organisatie?

Clean desk (Het zorgvuldig omgaan met bedrijfsgegevens en eigendommen, het opslaan of wegbergen daarvan bij afwezigheid)

- Is binnen uw organisatie een clean desk programma ontwikkeld?
- Worden medewerkers gewezen op het belang van een clean desk?
- Wordt de clean desk procedure regelmatig besproken tijdens het afdelingsoverleg?
- Is clean desk in de controleprogramma's opgenomen van het management en/of de accountantsdienst of de met controle belaste discipline?

Werving en selectie

- Wordt gebruik gemaakt van een psychologisch adviesbureau of een selectiebureau en zo ja, zijn afspraken gemaakt over:
  - o controle van het door de sollicitant opgegeven curriculum vitae?
  - o identificatie van de sollicitant?
  - o verificatie van het arbeidsverleden (voor zover deze activiteiten niet in tweede lijn door personeelszaken worden uitgevoerd)?
- Worden door het selectiebureau in geval van behandeling van vertrouwensfuncties, bijzondere criteria gesteld?
- Worden bij de wervingsactiviteiten alle facetten van de functiebeschrijving in de advertentie genoemd en kan er dan sprake zijn van een ongewenste vorm van informatieoverdracht?
- Wordt de sollicitant gevraagd middels een handgeschreven brief te reageren (om het handschrift van de sollicitant in het personeelsdossier vast te leggen)?
- Wordt de sollicitant een formulier voorgelegd, waarin naast de gebruikelijke vragen als personalia, gegevens van de naaste familie, gevolgde opleiding, arbeidsverleden e.d. de vraag wordt gesteld in hoeverre de betrokkene ooit in het verleden met politie of justitie in aanraking is geweest ter zake van het plegen van een misdrijf?
- Wordt de vraag over een mogelijk crimineel verleden per definitie altijd gesteld aan een sollicitant voor een vertrouwensfunctie?
- Dient de sollicitant voor een vertrouwensfunctie een 'bewijs van onbesproken gedrag' te overleggen?
- Moet de sollicitant zijn originele diploma's, getuigschriften e.d. tonen of kan hij ook volstaan met kopieën?
- Worden deze documenten op authenticiteit gecontroleerd?
- Vindt controle plaats van de door de sollicitant opgegeven opleidingen en behaalde titels?
- Worden de personalia van de sollicitant (in de eindfase) geverifieerd aan de hand van een geldig legitimatiebewijs (paspoort of rijbewijs)?
- Vindt er een huisbezoek plaats, teneinde een indruk te krijgen van het leefmilieu van de sollicitant?
- Wordt schriftelijk navraag gedaan bij de vorige werkgevers van de sollicitant?
- Zo nee, gebeurt dit door middel van een persoonlijk bezoek?
- Wordt voor sollicitanten van vertrouwensfuncties per definitie altijd een persoonlijk bezoek door of namens uw organisatie gebracht aan de voormalige werkgever(s)?
- Vindt er een controle plaats op een aaneensluitend arbeidsverleden? Indien 'zwarte gaten' in iemands arbeidsverleden worden ontdekt, vindt dan aanvullend onderzoek plaats?
- Let de bedrijfsarts of de keuringsarts bij de medische keuring op kenmerken die kunnen wijzen op mogelijk overmatig alcoholgebruik en/of gebruik van drugs?

Loopbaancontrole

- Indien de nieuwe werknemer in aanraking kan komen met gevoelige gegevens van de organisatie, moet hij dan vooraf een geheimhoudingsverklaring tekenen?
- Kan de nieuwe werknemer gedurende zijn proeftijd al kennis nemen van als vertrouwelijk of geheim gekwalificeerde informatie?

Loopbaancontrole (vervolg)

- Wordt gecontroleerd of werknemers de aan hen toegewezen verlofdagen, atv-dagen opnemen?
- Indien vanaf de werkvloer signalen worden opgevangen van overmatig alcoholgebruik of gebruik van verdovende middelen, worden deze dan ook gemeld aan de functionaris belast met de veiligheid?
- Is naast mogelijke bepalingen binnen de CAO een interne richtlijn opgesteld, die werknemers duidelijkheid verschaft over nevenbetrekkingen, commissariaten, adviseurschappen en dergelijke, die niet direct het bedrijfsbelang dienen?
- Is daarbij beoordeeld in hoeverre sprake kan zijn van een mogelijke vermenging van zakelijke en privébelangen?
- Is het werknemers toegestaan relatiegeschenken en dergelijke aan te nemen, die een bepaalde waarde te boven gaan?
- Wordt het declaratiegedrag van de werknemers periodiek aan een kritische controle onderworpen?
- Wordt in geval van gebruik van een bedrijfs- of leaseauto frequent onderzocht of er sprake is van een exorbitant hoog brandstofverbruik, waardoor men zou kunnen vermoeden, dat meer auto's op rekening van het bedrijf van brandstof worden voorzien?
- Indien een interne fraude of enige andere malversatie is ontdekt, wordt hiervan een rapport samengesteld en wordt van de dader een door hem te ondertekenen verklaring opgenomen?
- Indien hiervan aangifte zal worden gedaan, wordt dan eerst intern een uitvoerig onderzoek ingesteld?
- Wordt de politie in geval van een onderzoek verzocht geen persbericht van het onderzoek uit te geven?

Exitmaatregelen

- Geldt binnen uw organisatie de vaste regel, dat bij interne criminaliteit het dienstverband met de betrokken werknemer(s) wordt beëindigd?
- Zo ja, is deze regel bekend bij het personeel?
- Bestaan er procedures bij ontslag van de werknemer met betrekking tot het inleveren van:
  - o de bedrijfsauto?
  - o de hem/haar ter beschikking gestelde sleutels van het bedrijf?
  - o de hem/haar ter beschikking gestelde codes van kluizen?
  - o de hem/haar ter beschikking gestelde codes van geautomatiseerde systemen e.d. (deze dienen vervolgens terstond te worden gewijzigd)?
  - o de voor hem beschikbare gekwalificeerde informatie (de bedrijfsgeheimen)?
  - o overige bedrijfseigendommen?
- Worden bij het ontslag van de werknemer (of bij voorkeur kort daarvoor) diens bevoegdheden ingetrokken, zoals:
  - o betalingsopdrachten?
  - o kasopnames bij bank en/of giro?
  - o het zelfstandig afsluiten van contracten?

Tijdelijk personeel

• Zijn met de betrokken uitzendorganisatie(s) afspraken gemaakt over:
  o de controle op het door de uitzendkracht opgegeven curriculum vitae?
  o de controle en verificatie van de identiteit van de uitzendkracht?
o de aansprakelijkheid van de uitzendorganisatie?
• Worden uitzendkrachten, vakantiekrachten en stagiaires ook voor vertrouwensfuncties ingeschakeld/worden ze geplaatst op afdelingen/ locaties met een verhoogd criminaliteitsrisico?
• Tekenen tijdelijke arbeidskrachten een geheimhoudingsverklaring?
• Worden vakantiekrachten bij voorkeur uit familieleden van medewerkers van uw onderneming gerekruteerd?
• Indien stagiaires een scriptie of werkstuk samenstellen, kunnen zij daarin de als vertrouwelijk of geheim gekwalificeerde bedrijfsgegevens verwerken en publiceren?
• Dragen de tijdelijke arbeidskrachten in de organisatie zichtbaar een badge?
• Wordt bij gebruik van toegangscontrole de aanwezigheidsduur van betrokkenen geregistreerd en gecontroleerd?

Derdenbedrijven

• Vindt er een onderzoek plaats naar de kredietwaardigheid, de betrouwbaarheid en de continuïteit van de bedrijven die voor en/of binnen uw onderneming werkzaam zijn?
• Wordt gebruik gemaakt van slechts enkele derdenbedrijven of wordt periodiek het prijsniveau van deze bedrijven met dat van de concurrenten vergeleken?
• Mogen deze bedrijven ook bepaalde werkzaamheden privé voor medewerkers van uw onderneming verrichten of is het personeel toegestaan gebruik te maken van bepaalde faciliteiten van deze derdenbedrijven?
• Dragen de medewerkers van derdenbedrijven in de organisatie zichtbaar een badge?
• Wordt bij gebruik van toegangscontrole de aanwezigheidsduur van betrokkenen geregistreerd en gecontroleerd?

Bijlage 3 Negen tips bij interne fraude
Interne fraude wordt vaak gepleegd door leidinggevenden die al langer dan tien jaar bij een bedrijf werken. Wat kunt u doen om dit te voorkomen én wat als het toch gebeurt?

1. Zorg vooraf voor duidelijke regels
Het is van belang dat u duidelijke regels op schrift heeft over het gebruik van geld en goederen in uw organisatie. Zo kunt u bijvoorbeeld in uw huishoudelijk reglement opnemen dat gebruik van het geld van uw organisatie voor privédoeleinden niet, en ook niet tijdelijk, is toegestaan. Of dat betalingen aan werknemers nooit contant gebeuren, maar altijd via een bankbetaling. Op die manier kan fraude veel eenvoudiger worden bewezen.

2. Wie is het?
Een kant-en-klaar profiel van de dader bij u op kantoor bestaat niet geven, maar er zijn wel een paar statistische aanwijzingen. Daders van grote interne fraude zijn vaak loyale leidinggevenden die al langer dan tien jaar bij u in dienst zijn. Bijna driekwart van alle fraudeplegers is tussen de 35 en 55 jaar oud. Een derde van de fraudeurs werkt op de financiële afdeling en opvallend: een groot deel van de daders heeft een bestuurdersfunctie.

3. Zorg voor een duidelijke scheiding tussen betalen en autoriseren
Regel het zo dat er altijd, in ieder geval, een tweede persoon is, die meekijkt naar de mutaties op de betaalrekeningen. Met internetbankieren kan dat heel makkelijk.

Nog beter is het als u als regel hanteert dat de werknemer die de overboekingsopdrachten aan uw bank geeft, eerst een geautoriseerde betaalopdracht ontvangt van een chef of collega. Deze werknemer mag die betalingen dus alleen doen als een tweede persoon de factuur heeft gecontroleerd en een akkoord voor betaling heeft getekend. En de medewerker die de daadwerkelijke overboekingen doet, kan weer vaststellen of de door zijn collega of chef gegeven betaalopdrachten in orde zijn. Ondersteun deze scheiding tussen betalen en autoriseren door gebruik te maken van de functionaliteiten die het betaalpakket van uw bank biedt!

4. Houd controle en kijk mee
Degene die de betalingen autoriseert, moet na verwerking door de bank van de betaalopdrachten aan de hand van de dagafschriften (op papier of via beeldscherm) vaststellen dat er niet méér betalingen zijn verricht, dan waarvoor hij goedkeuring heeft gegeven.
Het is sowieso handig als meerdere mensen inzage in alle mutaties hebben. Als er dan toch fraude voorkomt, hebben deze personen immers ook inzage in alle mutaties en bent u minder afhankelijk van medewerking van de frauderende medewerker.
Het is wel belangrijk dat u zorgt dat de medewerker die in de gelegenheid is om te frauderen, nooit de bevoegdheid heeft om de instellingen van uw bankrekeningbeheer aan te passen. Anders zou hij bijvoorbeeld kunnen regelen dat u geen toegang meer heeft tot uw eigen rekening. Het beste is om deze bevoegdheid in uw eigen hand te houden.

5. Inzicht in uw administratie
Fraude wordt vaak gepleegd met contant geld, zoals een greep uit de kas of betalingen die niet worden geregistreerd. U kunt een paar dingen doen voor meer inzicht in uw administratie. Schaf het contante geldverkeer af of beperk dit. Zorg dat betalingen van en naar uw bedrijf uitsluitend per bank geschieden. Op die manier is er altijd zicht op de uitgaande en inkomende geldstroom. En in geval van nood kunt u snel een kopie van de bankadministratie op vragen bij uw bank.

6. Schep duidelijkheid
Geruchten, vermoedens en onrust onder uw personeel zijn slecht voor uw bedrijf. Heeft u eenmaal iemand in het vizier? Schep dan zo snel mogelijk duidelijkheid: is er sprake van fraude of niet? Ga een gesprek aan met de mogelijke fraudeur en vraag iemand uit uw bedrijf met financiële kennis om er bij te zitten.
Voer het gesprek in een vriendelijke sfeer. Op dit moment heeft u vragen, nog geen beschuldigingen. Er is een vervelende situatie ontstaan, die zo snel mogelijk moet worden beëindigd, zodat (ervan uitgaande dat er helemaal geen sprake is van fraude) de goede sfeer ook zo snel mogelijk wordt hersteld.

7. Sommeren of schorsen
Als het duidelijk is dat uw werknemer fraudeert, maar hij of zij wil niet meewerken en weigert inzage te geven bijvoorbeeld in de administratie, overweeg dan een formeel besluit om hem of haar te schorsen of te sommeren. Dat doet u per aangetekende brief. Daarin vermeldt u ook dat u aangifte doet van de fraude indien niet vóór een bepaalde datum en tijdstip aan de sommatie (het teruggeven van de administratie of andere bewijsstukken) is voldaan. In dit stadium is het verstandig om juridisch advies in te winnen.

8. Juridische stappen ondernemen?
U wilt het ontvreemde geld of de ontvreemde goederen terug, en onderneemt juridische stappen. Dat kan via het strafrecht (u doet dan aangifte bij de politie) of via een civiele procedure (u start zelf een rechtszaak).
In het wetboek van strafrecht is één en ander geregeld om fraude, of verduistering, diefstal of valsheid in geschrifte) te straffen. Een juridische procedure kost echter wel geld, tijd en energie. In veel gevallen is het te overwegen om te komen tot goede afspraken met de fraudeur om uw geld terug te krijgen.

9. Een bekentenis in ruil
Een manier om het zonder de rechter te regelen, is het maken van een afspraak of overeenkomst met de fraudeur. U vraagt van hem een schriftelijke bekentenis én een belofte om op korte termijn het ontvreemde bedrag terug te betalen. Uit deze bekentenis moet blijken voor welk bedrag is gefraudeerd en hoe de fraude in zijn werk is gegaan. De belofte om het ontvreemde bedrag terug te betalen moet vergezeld zijn van een concreet schema met bedragen en betalingsdata.