

2e bijeenkomst Ordina
7 maart 2022

Opleiding Inzicht in Witwassen en Fraude

Felix Olijslager



Programma van vandaag

Onderwerpen

- Fraude en aansprakelijkheid van de bank
- Het documenteren van fraude en integriteitsinbreuken door financiële instellingen
- Het PIFI en gegevensuitwisseling
- Afsluitende toets

Tijdsindeling

13.00 - 14.15: theorie fraude en aansprakelijkheid in drie delen
 14.15 - 14.30: pauze
 14.30 - 15.30: casus transactie-monitoring
 15.45 - 16.00: pauze
 16.00 - 17.00: theorie documenteren en bewaren in twee delen
 17.00 - 17.15: pauze
 17.15 - 17.45: casus gegevensuitwisseling
 17.45 - 18.30: eten
 18.30 - 19.15: Theorie EVR en Afsluitende toets



Financial Economic Crime

Verplichtingen wwft, wft en sanctiewetgeving

Wet ter voorkoming van witwassen en terrorismefinanciering (wwft)

- ▶ De Wwft beoogt de voorkoming van het gebruik van het financiële stelsel voor het witwassen van geld dat verkregen is uit criminele activiteiten.
- ▶ Dit is een algemeen maatschappelijk belang.
- ▶ Banken vervullen de rol van poortwachter.

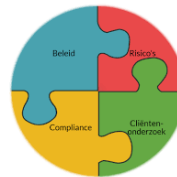
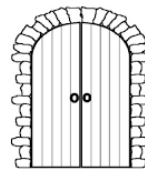


Poortwachtersfunctie



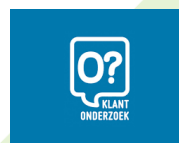
- De poortwachtersfunctie houdt in dat een bank ongewenste elementen in ons financiële stelsel waar nodig identificeert, weert en ongewenste transacties tegengaat of meldt.
- Banken zijn namelijk bij uitstek geschikt om aanwijzingen van witwassen te signaleren, omdat zij zicht hebben op de transacties van cliënten.
- Voor de poortwachtersfunctie is kennis van fraude- en witwasscenario's vereist.

De Poortwachter



Normering in de Wwft

- Artikel 3 Wwft: Een FI-instelling is verplicht om cliëntenonderzoek te verrichten ter voorkoming van witwassen en financieren van terrorisme.
- Artikel 5 Wwft: Een FI-instelling mag geen zakelijke relatie aangaan of een transactie uitvoeren, indien zij geen of geen bevredigend cliëntenonderzoek heeft verricht.
- Artikel 5 Wwft: Een FI-instelling is verplicht om een zakelijke relatie met een cliënt te beëindigen, indien de instelling niet kan voldoen aan het bepaalde in artikel 3, eerste en tweede lid, aanhef en onderdelen a, b, en c;



Normering in de Wwft

- Artikel 8 Wwft: Een FI-instelling is verplicht om in bepaalde gevallen een verscherpt cliëntenonderzoek te verrichten;
- Artikel 16 Wwft: Een FI-instelling is verplicht om ongebruikelijke transacties binnen twee weken onverwijld te melden aan de FIU nadat het ongebruikelijke karakter van de transactie kenbaar is geworden.



FIU

Strafbaarstelling in de Wed

- Overtredingen van de hiervoor genoemde Wwft-artikelen zijn op grond van artikel 2 lid 1 Wet op de economische delicten (WED) strafbaar gesteld als misdrijf.



Wet op het financieel toezicht



- Banken dienen hun cliënten te kennen én geen relaties aan te knopen met personen die het vertrouwen in de financiële onderneming kunnen schaden.
- Customer Due Diligence (CDD) is een hulpmiddel om dit te bewerkstelligen.
- De gevolgen van het niet beheersen van deze risico's kunnen het vertrouwen van de consument in de financiële onderneming schaden.



14 BPRWFT
3:10 Wft
3:17 Wft

Customer due diligence

CDD bestaat onder meer uit de onderdelen:

- acceptatie van cliënten
- identificatie en verificatie van cliënten
- indien van toepassing, de identificatie en eventueel verificatie van de uiteindelijke belanghebbende
- vaststellen van het doel en de beoogde aard van de zakelijke relatie
- monitoring en review van cliënten, rekeningen en transactie



Sanctiemaatregelen (1)



- Sanctiemaatregelen zijn politieke instrumenten in het buitenlands en veiligheidsbeleid van de Verenigde Naties en de Europese Unie.
- Het zijn dwingende, niet-militaire, instrumenten die worden ingezet als reactie op schendingen van het internationale recht of van mensenrechten door regimes die rechtsstatelijke en democratische beginselen niet eerbiedigen, in een poging een kentering teweeg te brengen.



Sanctiemaatregelen (2)

- Daarnaast vervullen sancties een rol in de bestrijding van terrorisme.
- Daartegen gerichte sancties zijn vooral gericht tegen individuen en niet-statelijke entiteiten.
- Sanctiemaatregelen berusten meestal op een resolutie van de VN-veiligheidsraad die vervolgens in secundair Europees recht worden omgezet.
- Een aantal sanctiemaatregelen heeft een autonome Europese grondslag.



Sanctiemaatregelen (3)



- De meest voorkomende sancties zijn:
 - wapenembargo's en handelsrestricties
 - financiële sancties (bevrozing tegoeden)
 - reis- en visumrestricties.



Transactiemonitoring Nederland (TMNL)

 Nederlandse Vereniging van Banken

Gezien hun rol van poortwachter spelen banken een belangrijke rol in de strijd tegen het witwassen van geld en de financiering van terrorisme in Nederland

Witwassen en terrorismefinanciering in NL


#8 in de top 10 landen die het aantrekkelijkst zijn voor witwassers
€16 MLD wordt jaarlijks witgewassen in Nederland

van het geld dat criminelen witwassen is afkomstig van drughandel en fraude **90%**
 van de gevallen van zorgfraude zijn gekoppeld aan terrorisme financiering **20%**




#1 witwasrisico, volgens deskundigen, is het witwassen van geld via banken
65% van alle criminaliteit heeft een financiële component via banken

Bron: FBI, NVB, WODC en OM

Poortwachterrol banken


8000 bankmedewerkers (meer dan 1 op de 10) zetten zich in voor de bestrijding van witwassen en financiering van terrorisme

waarschuwingen over mogelijke ongebruikelijke transacties werden gegenereerd door de banken in 2019 **>210k**


CAGR: +92% 
 155k
 Rapporten van banken van ongebruikelijke transacties ('MOTS' zijn gestegen)

Year	Number of Reports
2015	12k
2016	14k
2017	23k
2018	68k
2019	155k

Verschijningsvormen van fraude

en de relatie met de FEC-wetgeving

Het woord fraude

Het Wetboek van Strafrecht kent het woord "fraude" niet.

Wat kenmerkt fraude?

"Een opzettelijke handeling door een of meer personen waarbij misleiding wordt gebruikt om een onrechtmatig voordeel te behalen".

Vormen van misleiding, bedriegen, manipuleren en liegen zijn in verschillende artikelen in het Wetboek van strafrecht strafbaar gesteld.



Vaak is sprake van horizontale fraude

Dit is fraude waarbij de benadeelde een natuurlijke persoon of een privaatrechtelijke rechtspersoon is. De fraudeur is ook een natuurlijke persoon of rechtspersoon.

Dader

Particulier
Bedrijf
Particulier
Bedrijf

Slachtoffer

Particulier
Particulier
Bedrijf
Bedrijf

Juridische kwalificatie “fraude”

Verduistering - strafbaar gesteld in art. 321 WvSr

Valsheid in geschrifte - strafbaar gesteld in art. 225 WvSr

Verzwijging en/of liegen - strafbaar gesteld in art. 227a WvSr

Oplichting - strafbaar gesteld in art. 326 WvSr

Niet-ambtelijke corruptie – art. 328ter WvSr

Misbruik identiteit – art. 231, 231a, 231b WvSr

En vele andere artikelen die op specifieke situaties betrekking hebben.

Voorbeeld: oplichting art. 326 WvSr

Oplichting is strafbaar gesteld in art. 326 Wetboek van strafrecht:

Hij die, met het oogmerk om zich of een ander wederrechtelijk te bevoordelen,

Bewust,
opzettelijk

hetzij door het aannemen van een valse naam of van een valse hoedanigheid, hetzij door listige kunstgrepen, hetzij door een samenweefsel van verdichtfels,

de één
doet iets

iemand beweegt tot de afgifte van enig goed, tot het verlenen van een dienst, tot het ter beschikking stellen van gegevens, tot het aangaan van een schuld of tot het teniet doen van een inschuld, wordt, als schuldig aan oplichting, gestraft met gevangenisstraf van ten hoogste vier jaren of geldboete van de vijfde categorie.

waardoor
de ander
wordt
bewogen
tot iets

Er is een causaal verband tussen
de handeling van de bedrieger en
de handeling van het slachtoffer

Wat valt zoal onder oplichting?

- Beleggings- / investeringsfraude (Ponzi);
- Phishing met hyperlink naar valse website waar gegevens worden gevraagd;
- Phishing waarbij telefonisch om gegevens wordt gevraagd (helpdeskfraude);
- Hulpvraagfraude via WhatsApp;
- CEO-fraude;
- Marktplaatsfraude (indien doortrapt);
- Webwinkelfraude (namaakwebshops);
- Voorschotfraude (419 scams);
- Vakantiewoningen verhuurfraude;
- Factuurfraude (bepaalde varianten)
- Datingfraude (zie Netflix: Tinder Swindler).

Frauduleus verkregen geld wordt verplaatst via bankrekeningen en op deze manier komt de bijzondere zorgplicht van de bank in beeld.

Artikelen in het Wetboek van strafrecht naast 326 WvSr:

- Aquisitiefraude, art. 326d WvSr
- Fraude op online handelsplaatsen, art. 326e WvSr
- Flessentrekkerij, art. 326a WvSr

CEO-fraude



Voorschotfraude



Bijzondere zorgplicht van de bank

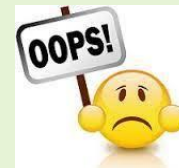
Geen criminele transacties faciliteren

Onrechtmatige daad (1)

Het faciliteren van criminele transacties is niet alleen in strijd met de Wwft, maar kan ook worden aangemerkt als “onrechtmatige daad”.

Artikel 6:162 Burgerlijk Wetboek

- Iemand die een onrechtmatige daad pleegt
- is verplicht de schade aan anderen te vergoeden
- als de onrechtmatige daad is toe te rekenen (een fout)
- mits er een oorzakelijk verband is tussen de schade en de fout.



Pleegt de bank een onrechtmatige daad als natuurlijke personen of rechtspersonen slachtoffer zijn van fraude?

Onrechtmatige daad (1)

Het faciliteren van criminele transacties is niet alleen in strijd met de Wwft, maar kan ook worden aangemerkt als “onrechtmatige daad”.

Artikel 6:162 Burgerlijk Wetboek

- Iemand die een onrechtmatige daad pleegt
- is verplicht de schade aan anderen te vergoeden
- als de onrechtmatige daad is toe te rekenen (een fout)
- **mits er een oorzakelijk verband is tussen de schade en de fout.**



Pleegt de bank een onrechtmatige daad als natuurlijke personen of rechtspersonen slachtoffer zijn van fraude?



Casus windenergie (1)



Met beleggingsproducten is geld opgehaald voor investeringen in vastgoed in windenergie door het bedrijf Nieuwe Hollandsche Wind. Er was sprake van beleggingsfraude. De uitbaters zijn vervolgd voor oplichting, verduistering en witwassen.

De curator van het failliete bedrijf Nieuwe Hollandsche Wind sleept Knab voor de rechter. Volgens de curator blokkeerde de bank veel te laat een bankrekening van het bedrijf. Zo konden de van frauduleuze uitbaters van het bedrijf zo'n 600.000 euro wegsluizen.

Belang van de casus: Is er een oorzakelijk verband tussen de schade en een fout van de bank?



Casus windenergie (2)



Nieuwe Hollandsche Wind stortte ongeveer zes ton op de rekening van Valeo Media. Dat was de privéonderneming van de 36-jarige Stefan S, één van de hoofdverdachten in de strafzaak.

Op het moment van die overboekingen was Valeo Media al tijden failliet en werd daarna zelfs ontbonden. Het bedrijf bestond dus niet meer.

Maar de bankrekening die bij de onderneming hoorde, was na het faillissement door Knab niet geblokkeerd. Dat zou pas driekwart jaar na de ontbinding zijn gedaan, zegt de curator. Zo was er nog tijd om het geld over te hevelen. Vanaf de rekening van Valeo Media werd het geld verder doorgeboekt.



Casus windenergie (3)



De curator: “Een bank moet volgens hem wijzigingen in het handelsregister zien. Dan moet er een rood lampje gaan knippenen.”

De bank is volgens de curator aansprakelijk tegenover Nieuwe Hollandsche Wind. Met de schadevergoeding hoopte hij dat beleggers nog iets terugzien van hun inleg.



Casus windenergie (4)



De rechter*:

Voor vestiging van aansprakelijkheid (en daarmee voor het ontstaan van een wettelijke verplichting tot vergoeding van schade) is een **oorzakelijk verband** nodig tussen de vermeende fout van Knab en de schade. Dat **ontbreekt in deze zaak**.

De curator heeft niet aannemelijk kunnen maken dat, ook al had Knab bij het uitspreken of opheffen van het faillissement de Knab-rekening opgeheven of geblokkeerd, daarmee de schade bij de schuldeisers van zelf was voorkomen.

Het is immers niet uitgesloten dat de gelden ook naar andere bankrekeningen dan de Knab-rekening hadden kunnen worden overgemaakt en van daar kunnen worden door geboekt.



*Rechtbank Den Haag 11 september 2019, ECLI:NL:RBDHA:2019:9579

Onrechtmatige daad (2)

De onrechtmatigheid kan bestaan in de volgende normovertredingen:

- a. Een inbreuk op een recht van een ander;
- b. Een doen of nalaten in strijd met een wettelijke plicht;
- c. Een doen of nalaten in strijd met hetgeen volgens ongeschreven recht in het maatschappelijk verkeer betaamt.



Casus Winterswijk



In de crediteurenadministratie van de gemeente heeft een ambtenaar geld van de gemeente verduisterd door rekeningnummers van bestaande crediteuren van de gemeente te vervangen door rekeningnummers van zijn eigen ondernemingen (2 bakkerijen, 2 lingeriezaken en een muziekzaak).

Op deze wijze hebben 38 betalingen plaatsgevonden op bankrekeningen bij Rabobank, als gevolg waarvan de bankrekening van de gemeente voor in totaal voor een bedrag van € 2.682.468,52 is gedebiteerd.

Hoe ver gaat de zorgplicht van de bank als een werknemer geld verduistert van zijn werkgever?



Stelling gemeente Winterswijk



“Rabobank was de huisbankier van de frauderende ambtenaar en diens ondernemingen.

Gezien haar positie in het girale betalingssysteem had de Rabobank bepaalde controles dienen te verrichten, te weten controle van ongebruikelijke transacties en transactiepatronen, alsmede een naam/nummercontrole.

Door dit na te laten heeft zij de bijzondere zorgplicht geschonden en is Rabobank aansprakelijk voor de door de gemeente geleden schade.”



Hoe ver gaat de zorgplicht van de bank?

Uit de jurisprudentie van de Hoge Raad (Safe Haven)* volgt:

“De maatschappelijke functie van banken brengt een bijzondere zorgplicht met zich mee.

Dit geldt zowel jegens cliënten van de bank uit hoofde van de contractuele relatie, als ten opzichte van derden met wier belangen de bank rekening behoort te houden op grond van hetgeen in het maatschappelijk verkeer betaamt.

De reikwijdte van deze bijzondere zorgplicht hangt af van “de omstandigheden van het geval.”

Schending van de zorgplicht is een onrechtmatige daad.

Onrechtmatige daad (3)

Wat zegt het leerstuk van de onrechtmatige daad ook:

Eigen schuld van het slachtoffer wordt verrekend:

Een partij die wordt aangesproken wegens geleden schade, kan zich op de eigen schuld van de benadeelde beroepen en zo proberen de door hem te betalen schadevergoeding te verminderen (artikel 6:101 lid 1 BW)

Oordeel rechter Winterswijk



In navolging van de rechtbank concludeert het gerechtshof * dat de AO/IC van de gemeente Winterswijk niet deugde:

Er was onvoldoende functiescheiding en onvoldoende verificatie (validatie) van beoogde en reconciliatie van uitgevoerde betalingen.

De gemeente heeft ook eigen schuld aan de kwestie. Er is sprake van zodanige tekortkomingen in de AO/IC dat de bankgeen verwijt kan worden gemaakt. Rabobank niet aansprakelijk voor de schade.



* Gerechtshof Arnhem-Leeuwarden, 28 oktober 2014: ECLI:NL:GHARL:2014:8246

Strijd met een wettelijke plicht

De onrechtmatigheid kan bestaan in de volgende normovertredingen:

- a. Een inbreuk op een recht van een ander;
- b. Een doen of nalaten in strijd met een wettelijke plicht;**
- c. Een doen of nalaten in strijd met hetgeen volgens ongeschreven recht in het maatschappelijk verkeer betaamt.

Wanneer is sprake van een doen of nalaten in strijd met een wettelijke plicht? Het antwoord is van belang in relatie tot de FEC-wetgeving.



Casus Varta



Varta bankiert bij Commerzbank in Duitsland.

Een administratief medewerkster van Varta heeft vijf betalingsopdrachten voorbereid voor bankoverschrijvingen van de bankrekening van Varta naar het bankrekeningnummer van haar zus (die bij ABN AMRO bankiert), maar onder opgave van namen van klanten van Varta.

Deze medewerkster had zelf geen autorisatie om betalingsopdrachten te laten uitvoeren. Nadat zij de opdrachten had voorbereid, dienden deze door een gemachtigde medewerker te worden geautoriseerd.

De vijf betalingsopdrachten, voor in totaal € 129.263,90 zijn uitgevoerd.



Casus Varta



Volgens een interne procedure van ABN AMRO wordt (of werd ten tijde van dit voorval) van nationale en internationale betalingsopdrachten vanaf een bedrag van € 15.000,- ten gunste van een klant van ABN AMRO handmatig gecontroleerd of het rekeningnummer overeenstemt met de naam van de begunstigde.

Onderzoek door de afdeling Security Integrity Management (SIM) brengt de fraude weliswaar aan het licht, maar dat kon niet voorkomen dat het geld van een aantal transacties niet meer kon worden tegengehouden.



Stelling van Varta



“Als ABN AMRO de naam-nummercontrole had uitgevoerd dan had zij gezien dat de naam van degene ten aanzien van wie de betaling werd gedaan niet klopte met de naam van hun begunstigde rekeninghouder. Dan zou zij de frauduleuze betalingen hebben geconstateerd en dan zou (verdere) schade kunnen zijn voorkomen.

Door naam/nummercontrole na te laten heeft zij de bijzondere zorgplicht geschonden en is AA aansprakelijk voor de door Varta geleden schade.”

Oordeelrechter



Rechtbank Amsterdam* : ABN AMRO is niet aansprakelijk.

“ABN AMRO heeft geen verplichting om een naam / nummercontrole uit te voeren. In artikel 7:542 BW is vastgelegd, dat wanneer een betaalopdracht wordt uitgevoerd op basis van een unieke identificator, zoals in dit geval een bankrekeningnummer, de betaalopdracht geacht wordt correct te zijn uitgevoerd wat betreft de in dat nummer gespecificeerde begunstigde.

Op grond van het bepaalde in artikel 7:537 BW heeft ABN AMRO voorts de plicht betalingsopdrachten terstond te verwerken.

Onrechtmatige daad (4)

Relativiteitsbeginsel (Artikel 6:163 BW):

“geen verplichting tot schadevergoeding bestaat wanneer de geschonden norm niet strekt tot bescherming tegen de schade zoals de benadeelde die heeft geleden.”

Casus Palm Invest



Danny Klomp en Remco Voortman gebruikten de inleg in Palm Invest onder meer voor de aankoop van villa's, auto's en boten. Ook gaven de heren tienduizenden euro's uit bij een juwelier. Ze pinden met een pasje van de bankrekening van Palm Invest. De investeerders zijn uiteindelijk € 24 miljoen kwijt.

De bankrekening van Palm Invest werd beheerd door ABN Amro.

Volgens de curator had ABN Amro argwaan moeten krijgen bij de opmerkelijke transacties die via de AA-rekening zijn gedaan. Indien AA in het kader van haar CDD-verplichting beter toezicht had gehouden, dan was de schade/schuld van Palm Invest ten opzichte van haar schuldeisers vele malen kleiner.

Oordeel rechter



Rechtbank Amsterdam*: ABN AMRO is niet aansprakelijk

“CDD is niet bedoeld ter bescherming van de belangen van individuele cliënten van banken.

De in de Wft neergelegde CDD-normen beogen de integriteit en betrouwbaarheid van het financiële stelsel en van afzonderlijke banken te waarborgen”.

Individuele cliënten van banken kunnen dan ook geen aanspraken ontlenen aan eventuele schending van die normen (artikel 6:163 BW-relativiteitsbeginsel).



Rechtbank Amsterdam 8 november 2012, ECLI:NL:RBAMS:2012:BY2758

Casus Golden Sun Resorts



Een bijna meesterlijke zwendel”, zo wordt het investeringsproject Golden Sun (een luxe vakantieresort in Turkije) genoemd. Meer dan 650 beleggers hebben hun geld geïnvesteerd in dit luchtkasteel. Geld dat (deels) verdween in gokpaleis Holland Casino.

De bankrekening van makelaars- en beleggingskantoor Hooghuys en Versteeghe werd beheerd door ABN Amro.

Gedupeerden van de zwendel klagen ABN AMRO aan. Volgens de beleggers heeft de bank onrechtmatig gehandeld door na te laten onderzoek te doen naar de gang van zaken, beleggers te waarschuwen en bankrekeningen van te blokkeren toen haar duidelijk behoorde te zijn dat sprake was van beleggingsfraude.



Wat heeft AA wel gedaan? (1)



Op 15 juni 2007 heeft een medewerker van de bank aan de accountmanager en aan afdeling Compliance van de bank melding gemaakt van een ongebruikelijke transactie op de bankrekening.

De accountmanager heeft de gang van zaken op de rekening regelmatig bekeken. Hij signaleerde dat op de rekening bedragen binnen komen van 50K (minimale inschrijving) of een veelvoud daarvan en dat gelden naar Turkije gaan voor bouwactiviteiten en dat uitkeringen worden gedaan aan obligatiehouders.

Hij concludeert dat er geen direct wantrouwen was ten aanzien van de klant. De uitgevoerde transacties zijn niet ongebruikelijk bij investeringsprojecten.



Wat heeft AA wel gedaan? (2)



Begin augustus 2007 wordt naar aanleiding van een melding van Holland Casino aan de bank vastgesteld dat door Marc de B. diverse keren contant geld was opgenomen bij Holland Casino – uiteindelijk - ten laste van de rekening van de klant.

Er wordt onderzoek gedaan door SIM, compliance en JZ.

De bestuurders zijn niet bereikbaar voor de bank en verschijnen niet op gemaakte afspraken. De rekening wordt geblokkeerd en de relatie wordt opgezegd.

Zie voor andere vergelijkbare zaken:

<https://www.gelderlander.nl/home/klokkenluider-over-frauduleuze-beleggers-zuipen-snuiven-feesten~a020fa29/?referrer=https://www.google.com/>



Oordeel rechter



Rechtbank Amsterdam*

“Van aansprakelijkheid kan sprake zijn in geval van **subjectieve wetenschap** dat een rekeninghouder van de bank anderen oplicht, terwijl een adequate reactie van de bank uitblijft, zoals onderzoek en analyse van het rekeningverloop en het confronteren van de rekeninghouder als het ongebruikelijke verloop van de rekening wordt vastgesteld”.

Geen aansprakelijkheid van ABN AMRO omdat die subjectieve wetenschap van fraude pas ontstond van de melding van Holland Casino over contante opnamen ten laste van de rekening en AA vervolgens adequaat heeft gehandeld.



* Rechtbank Amsterdam 10 september 2014: ECLI:NL:RBAMS:2014:8484

Wat is wetenschap?

Wetenschap van de bank met betrekking tot ongebruikelijke betalingsverkeer:

“Wetenschap is een intern proces bij (medewerkers van) de bank en moet aan de hand van objectieve feiten en omstandigheden worden vastgesteld.

In die zin gaat het om geobjectiveerde wetenschap.

Het gaat om of de bank moet hebben geweten dat op de rekeningen ongebruikelijk betalingsverkeer plaatsvond.”



* Gerechtshof Den Haag d.d. 18 maart 2014, rol. nr: 334313 / HAZA09-1869

Voorlopige conclusies

Als derden gedupeerd worden door een rekeninghouder van de bank *kan* sprake zijn van aansprakelijkheid van de bank als de bank:

“niet adequaat reageert op een patroon van afwijkende en ongebruikelijke betalingen, nadat de bank hiervan wetenschap heeft verkregen.”



Zie voor een zeer uitvoerige bespreking van zorgplicht: ECLI:NL:PHR:2015:1975

Wat is adequaat reageren?

Een medewerker van de bank moet een bepaald soort gedrag vertonen, bijvoorbeeld:

- iets onderzoeken
- iemand informeren of waarschuwen
- De klant om opheldering vragen
- weigeren om een opdracht uit te voeren
- zich niet laten afschepen



Essentiele vraag

Is een bank jegens derden aansprakelijk als een rekeninghouder van de bank (fraudeur of katvanger) op diens rekening van fraude afkomstig geld ontvangt en uit geeft, opneemt, laat opnemen of door boekt naar ander rekeningnummer?

Denk aan factuurfraude, CEO-fraude of voorschotfraude.

Hiervan zijn vaak natuurlijke personen en bedrijven slachtoffer die geen enkele relatie met de bank hebben. Zij zijn zelf geen rekeninghouder.

We gaan deze vraag beantwoorden aan de hand van een casus, waarmee jullie zelf aan de slag gaan.



Casus – Foot Locker



Casus:

Verdachte registreert zich met een eenmanszaak, met de naam Ups Consultancy bij de Kamer van Koophandel (werkzaam in de sfeer van coaching) en opent een zakelijke rekening bij ING.

Foot Locker is een internationaal detailhandelsbedrijf en maakt gebruik de koeriersdiensten van UPS.

Foot Locker ontvangt een “request of change” voor het wijzigen van het rekeningnummer van UPS waarop Foot Locker de rekeningen van UPS betaalde.



Tussen 15 januari en 26 februari heeft Foot Locker in wekelijkse betalingen in totaal ruim € 1.800.000 naar de rekening van “Ups” overgemaakt. Er worden overboekingen gedaan naar een buitenlandse rekening en er worden contante opnamen gedaan.



Vervolg casus – Foot Locker



Vervolg casus:

Op 25 en 28 januari en 3 februari is bij ING ten aanzien van transacties op de rekening van Ups een “alert” gegeven. De alerts worden op de afdeling Klantmonitoring gegenereerd vanuit het post-events transactiemonitoringssysteem.

Naar aanleiding van alerts op deze transacties stelt ING een onderzoek in. Dit resulteert in een melding van verdachte transacties bij FIU op 5 februari omdat de transacties niet passen bij een coaching bureau.

FIU

Aan de rekeninghouder heeft ING vragen gesteld die niet beantwoord worden. Er wordt niet aangedrongen. Pas na een fraudemelding van Foot locker blokkeert ING de rekening.



Vervolg casus Foot Locker



Foot Locker doet aangifte tegen de rekeninghouder ter zake van onder meer oplichting, verduistering en witwassen.

De verdachte wordt veroordeeld voor schuldwitwassen.

Foot Locker stelt ING aansprakelijk voor de door haar geleden schade. Foot Locker verwijt ING dat het niet heeft ingegrepen.

Terzijde:

Bij vonnis van deze rechtbank is verdachte vanwege schuldwitwassen veroordeeld tot onder meer betaling van ruim € 1,8 miljoen aan Foot Locker als benadeelde partij.



Oordeel rechtbank



- Foot locker is weliswaar geen rekeninghouder van ING, maar de maatschappelijke functie van de bank brengt een bijzondere zorgplicht met zich mee. Dat betekent dat rekening moet houden met de belangen van derden op grond van hetgeen volgens ongeschreven recht in het maatschappelijk verkeer betaamt.
- Voor een schending van de zorgplicht jegens een derde is **subjectieve wetenschap vereist** van (medewerkers van) de bank ten aanzien van het ongebruikelijke verloop van transacties op de rekening van een frauderende rekeninghouder.
- **Na de drie alerts van ongebruikelijke transacties was ING zich bewust van de ongebruikelijke activiteiten op de rekening van Ups.**
- **Dat blijkt ook wel uit het feit dat een melding bij het FIU is gedaan.**



Rechtbank Amsterdam, 26 juli 2017: ECLI:NL:RBAMS:2017:5360

Oordeel rechtbank vervolg



- Voor de medewerkers die zich met het dossier bezig hielden, moest duidelijk zijn dat – indien sprake was van fraude – de schade voor de benadeelde snel zou oplopen. Zij hadden adequaat moeten optreden!
- ING heeft weliswaar onderzoek gedaan, en is dus niet blijven stilzitten, maar zij is daarbij, gelet op de omstandigheden van dit geval, onvoldoende voortvarend te werk gegaan.



Rechtbank Amsterdam, 26 juli 2017: ECLI:NL:RBAMS:2017:5360

Oordeel gerechtshof



Later zegt het gerechtshof in hoger beroep:

ING had op 25 januari bij de 1e alert al nader onderzoek moeten doen naar de ongebruikelijke transacties.

Het gerechtshof is van oordeel dat ING na de tweede alert op 28 januari de rekening van Ups onmiddellijk had moeten blokkeren en derhalve de betalingsopdrachten van Ups had moeten weigeren.



Gerechtshof Amsterdam, 14 mei 2019: ECLI:NL:GHAMS:2019:1611

Oordeel gerechtshof



- De verdenkingen van fraude waren toen zo concreet dat ING, vooruitlopend op de uitkomst van het op 25 januari 2015 gestarte onderzoek, onmiddellijk mocht en moest ingrijpen. Voor het mogen weigeren van betaalopdrachten is een vermoeden van onregelmatigheden reeds voldoende (zie rov. 2.14).
- Voor het gerechtshof is ook niet duidelijk waarom ING geen navraag heeft gedaan bij Foot Locker.
- De schade van Foot Locker bestaat uit de bedragen die vanaf 29 januari van de rekening van Ups zijn afgeschreven, in totaal een bedrag van € 1.004.507,50.



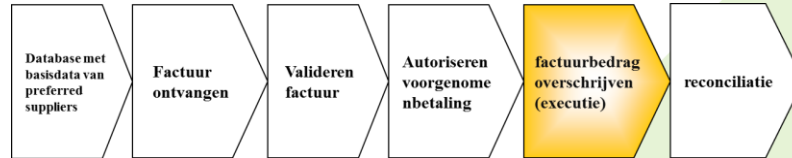
Gerechtshof Amsterdam, 14 mei 2019: ECLI:NL:GHAMS:2019:1611

Ook Foot Locker was nalatig



De rechter stelt ook vast:

- dat Foot Locker ook nalatigheid kan worden verweten doordat zij haar interne administratieve proces niet op orde had.



- Rechtbank en hof oordelen dat partijen in gelijke mate hebben bijgedragen aan het ontstaan van de schade, zodat er aanleiding is om de vergoedingsplicht van ING op grond van eigen schuld aan de zijde van Foot Locker te verminderen met 50 procent. De billijkheid vereist naar het oordeel van de rechtbank geen andere verdeling van de schade.

Gevolg: ING moet € 502.253,75 aan Foot Locker betalen en voor het restant van de schade moet Foot Locker op de blaren zitten.

Casus Rotterdams Havenbedrijf



Casus:

Het Havenbedrijf is in publieke handen. De gemeente Rotterdam bezit 70 procent van de aandelen; de Nederlandse staat de resterende 30 procent.

In 2018 werd het Havenbedrijf opgeschrikt door een omvangrijke fraude door een leidinggevende. De man zorgde ervoor dat het Havenbedrijf dertien rekeningen van een bedrijf van zijn neef (FMS Group) van in totaal € 457.319,50 betaalde, terwijl daar niets tegenover stond.

Casus Rotterdams Havenbedrijf



Modus operandus

Het (waarnemend) afdelingshoofd D&IT [verdachte 1] heeft een collega benaderd voor het aanmaken van een nieuwe leverancier - FMS - in het SAP-systeem van het Havenbedrijf.

Hij verzocht daarbij om dit 'onder de radar', buiten het zicht van de inkoopafdeling van het Havenbedrijf, te houden.



Rechtbank Amsterdam 23 oktober 2019: ECLI:NL:RBAMS:2019:7887

Casus Rotterdams Havenbedrijf



Nadat FMS op die wijze in het 'SAP-systeem' was aangemaakt als nieuwe leverancier, heeft verdachte één zijn ondergeschikte collega's herhaaldelijk geïnstrueerd om ten behoeve van FMS zogenoemde 'inkooporders' (IO's/PO's) aan te maken voor inhuur van personeel.

Deze inkooporders heeft hij iedere keer vrijgegeven, waarna hij zijn collega's steeds heeft verzocht om zogenoemde 'prestatieboekingen' in het SAP-systeem van Havenbedrijf te doen, zodat zijn ondergeschikten hem vervolgens de 'ordernummers' en 'sif-nummers' konden toezenden.

Die nummers gaf verdachte 1 aan FMS door, zodat FMS deze op haar facturen aan het Havenbedrijf kon vermelden om de betreffende facturen door het Havenbedrijf betaald te krijgen tussen eind 2016 en het eerste kwartaal van 2018.



Rechtbank Amsterdam 23 oktober 2019: ECLI:NL:RBAMS:2019:7887

Hoe is de zaak ontdekt?



Ten laste van de bankrekening die FMS aanhield bij ING zijn gedurende een bepaalde periode door de neef van verdachte 1 telkens geldbedragen van telkens 10.000 euro gepind bij verschillende bankfilialen van ING.

Op basis daarvan heeft ING FMS om opheldering gevraagd. Verdachte 1 is toen in paniek geraakt en heeft een valse inhuurovereenkomst opgesteld tussen het Havenbedrijf en FMS en deze aan ING toegezonden.

De betalingen van het Havenbedrijf aan FMS waren de enige 'zakelijke' inkomsten van FMS. Verder zijn er vanaf de bankrekening van FMS alleen privébetalingen verricht en geen zakelijke betalingen, zoals betalingen van salaris aan medewerkers of ingehuurde krachten.

ING heeft de geldigheid van deze inhuurovereenkomst vervolgens geverifieerd bij het Havenbedrijf, waarna de zaak aan het licht kwam.



Rechtbank Amsterdam 23 oktober 2019: ECLI:NL:RBAMS:2019:7887



Incidentenwaarschuwingssysteem

PIFI, verwerken van persoonsgegevens en gegevensuitwisseling

Omgaan met persoonsgegevens

- Op Europees niveau geldt vanaf 25 mei 2018 de AVG.
- In Nederland worden in de Uitvoeringswet AVG (UAVG) aanvullingen beschreven, die mogelijk zijn omdat de AVG daarvoor ruimte biedt aan de landen in Europa.
- Daarnaast zijn er sectorspecifieke wetten in Nederland die bepalingen bevatten over het verwerken van persoonsgegevens.



Wanneer is de AVG van toepassing?

Geautomatiseerd verwerken van persoonsgegevens



Wat is een persoonsgegeven?

Een persoonsgegeven is elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon.



8.	Verzekeringsmaatschappij (zie verzekeringspolis)
NAAM:
Polisnr.:
Groene kaart nr.:
Verzekeringspolis of groene kaart geldig	

AVG / GDPR

Wat is “verwerken”?

- Het gehele proces dat een persoonsgegeven doormaakt vanaf het moment van verzamelen tot en met het moment van vernietigen.
- De AVG noemt onder meer het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken en verstrekken van persoonsgegevens.

AVG / GDPR

Verwerken van
PERSOONSgegevens

Daarmee is de AVG van toepassing op:

- Het uitwisselen van klantgegevens met anderen (intern en extern)
- het opslaan van ID-bewijzen
- het onderzoeken van mogelijke inbreuken op veiligheid en integriteit
- vastleggen persoonsgegevens in het incidentenregister
- vastleggen van camerabeelden en vastleggen gegevens in een toegangsbeheersingssysteem
- Screening op sanctielijsten/PEP-check



AVG als algemeen Europees kader

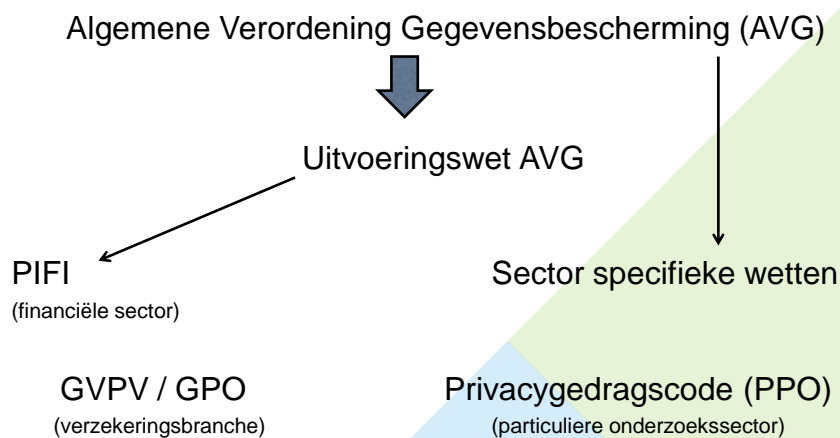
- De AVG geeft het Europese kader voor de omgang met persoonsgegevens. De AVG bevat veel open normen.
- Dat betekent dat de AVG met het oog op de toepassing in de praktijk op tal van punten nader moet worden ingevuld en geoperationaliseerd.



AVG als algemeen Europees kader

- In veel sectorale wetten is beschreven wanneer en onder welke voorwaarden “bijzondere persoonsgegevens” mogen worden verwerkt en zijn bepalingen vastgelegd over gegevensuitwisseling.
- Ook heeft nadere invulling en operationalisering plaatsgevonden in onder meer
 - de Gedragscode Verwerking Persoonsgegevens Verzekeraars;
 - de Privacygedragscode van de Nederlandse Veiligheidsbranche en het
 - het Protocol Incidentenwaarschuwingssysteem financiële instellingen (Pifi).

Nadere invulling van de AVG



Daarnaast de Wet politiegegevens, en de Wet justitiële en strafvorderlijke gegevens die gebaseerd zijn op een Europese richtlijn. ¹¹

Twee onderzoeksadministraties

Voor het vastleggen van gegevens over fraude, veiligheid en integriteit kent een FI twee onderzoeksadministraties:

Een onderzoeksadministratie is een logisch geheel van (gedigitaliseerde) documenten en informatie en heeft betrekking op een zaak, een persoon of een kwestie.

Gebeurtenissenadministratie

Incidentenregister

Gebeurtenissenadministratie

Verschillende categorieën van gebeurtenissen: in de gebeurtenissenadministratie:

- Overheidsbevragingen
 - FIU-meldingen
 - CDD-informatie
- } Gegevens komen uit de klantenadministratie
- Employmentscreening
- } Gegevens komen uit personeelsadministratie
- Fraudemeldingen
- } "Incidenten" zoals gedefinieerd in het PIFI. Een gebeurtenis is een incident als VZ dat bepaalt.

Signalen van buitenaf die aandacht vragen van de financiële instelling:

Tips van cliënten en relaties, Meld Misdaad Anoniem, overheidsbevragingen, informatie van politie etc.

Gebeurtenissenadministratie van de afdeling Veiligheidszaken of een aangewezen afdeling van de financiële instelling, belast met fraude, veiligheid en integriteit

Registratie van gegevens ten behoeve van de veiligheid en integriteit.

(GA maakt deel uit van het verwerkingsregister van de FI)

Signalen vanuit (de diverse administraties binnen de bedrijfsprocessen van) de financiële instelling:

Zoals ongebruikelijke transacties, CDD en signalen van mogelijke overtredingen van gedragscodes, alsmede meldingen medewerkers

Persoonsgegevens in de GA worden NIET gedeeld met andere financiële instellingen

Verzameldoel van persoonsgegevens in GA

“Het ondersteunen van het geheel aan activiteiten die gericht zijn op het waarborgen van de veiligheid en de integriteit **van de financiële instelling, de economische eenheid (groep) waartoe de FI behoort, haar cliënten en medewerkers**, daaronder mede begrepen (het geheel van) activiteiten die gericht zijn:

- op het onderkennen, voorkomen, onderzoeken en bestrijden van **ongewenste gedragingen**;
- op het onderkennen, voorkomen, onderzoeken en bestrijden van **oneigenlijk gebruik van producten, diensten en voorzieningen en/of (pogingen tot) strafbare of laakbare gedragingen en/of overtreding van (wettelijke) voorschriften**.

UITSLUITEND VOOR INTERN GEBRUIK



Gebeurtenissenadministratie

Bepaalde gebeurtenissen kunnen voor de financiële instelling aanleiding zijn om bij dienstverlening of indienstneming extra alert te zijn ten aanzien van de bij gebeurtenis betrokken personen.

Om die reden kan aan die gebeurtenissenadministratie een Intern Verwijzingsregister (“IVR”) worden gekoppeld waarmee het mogelijk is om frontoffices en HR-afdelingen te alerteren op die (rechts)personen.

Het IVR bevat uitsluitend Verwijzingsgegevens.

Omdat er verschillende categorieën van gebeurtenissen zijn, zijn er ook verschillende categorieën van interne verwijzingen.

Sommige categorieën van gebeurtenissen mogen niet gedeeld worden met de frontoffices en HR-afdelingen vanwege wettelijke geheimhoudingsbepalingen

Zoals FIU-meldingen en vorderingen van opsporingsinstanties.

IVR

Categorieën van gebeurtenissen die wel kunnen worden opgenomen. Dan worden verwijzingsgegevens opgenomen van bijvoorbeeld:

- Wanbetalers
- Degenen die zich schuldig hebben gemaakt aan een incident
- Personen tegen wie een onderzoek loopt, mits redelijk vermoeden van betrokkenheid
- Personen met negatief CDD



Autorisatiematrix

Binnen een financiële instelling zijn doorgaans meerdere afdelingen belast met het beheersen van fraude, veiligheid en integriteit.

Al deze afdelingen kunnen werkzaam zijn met hetzelfde softwarepakket.

Je hebt een autorisatiematrix nodig dat taakgerichte bevoegdheden en toegang inregelt en wat vervolgens softwarematig ondersteund en afgedwongen moet worden.

Kenmerken Gebeurtenissenadministratie

Geen regulering door de branchevereniging

1. Iedere financiële instelling bepaalt zelf welke categorieën van gebeurtenissen zich lenen voor opname in het IVR, waarbij ook de opnamecriteria per instelling kunnen verschillen.
2. De bewaarduur kan per categorie van gebeurtenis verschillen.
3. Per categorie van gebeurtenis moet worden nagedacht over het al dan niet informeren van de betrokkene dat diens gegevens zijn vastgelegd in de GA.

Incidentenregister



Gegevens uit het Incidentenregister kunnen worden uitgewisseld met de functionarissen van Veiligheidszaken van andere financiële instellingen en de fraudeloketten van de brancheverenigingen (4.2.2. en 4.2.3 PIFI).

Incidentenregister Veiligheidszaken

In het Incidentenregister worden gegevens vastgelegd van (mogelijke) Incidenten.

Een incident is een gebeurtenis die als gevolg heeft, zou kunnen hebben of heeft gehad dat de belangen, integriteit of veiligheid van de cliënten of medewerkers van een financiële instelling, de financiële instelling zelf of de financiële sector als geheel in het geding zijn of kunnen zijn,

Voor opname van gegevens moet worden voldaan aan de verzameldoelen voor het Incidentenregister die genoemd zijn in artikel 4.1.1. van het PIFI.

De gegevens in het Incidentenregister zijn alleen toegankelijk voor medewerkers van Veiligheidszaken

Gegevens in het Incidentenregister worden niet langer bewaard dan 8 jaar na het moment van eerste vastlegging van die gegevens (paragraaf 4.3 PIFI).

Doelstelling vastlegging gegevens in IR

“Het ondersteunen van activiteiten gericht op het waarborgen van de veiligheid en de integriteit van de financiële instelling (FI), daaronder mede begrepen (het geheel van) activiteiten die gericht zijn:

- op het onderkennen, voorkomen, onderzoeken en bestrijden van gedragingen die kunnen leiden tot benadeling van de FI;
- op het onderkennen, voorkomen, onderzoeken en bestrijden van oneigenlijk gebruik van producten, diensten en voorzieningen en/of (pogingen tot) strafbare of laakbare gedragingen en/of overtreding van (wettelijke) voorschriften, **gericht tegen de branche waar FI deel van uitmaakt**, de economische eenheid (groep) waartoe de FI behoort, de FI zelf, haar cliënten en medewerkers **en (facultatief)**;
- **het gebruik van en de deelname aan waarschuwingssystemen.”**

Softwarematige ondersteuning

Voor beide onderzoeksadministraties kan hetzelfde softwarepakket gebruikt worden.

Verschillende marktpartijen bieden dit soort softwarepakketten aan.

Met deze software kunnen op effectief wijze verschillende deelbestanden op kenmerken, zoals een naam, doorzocht kunnen worden.



Pega (ING)

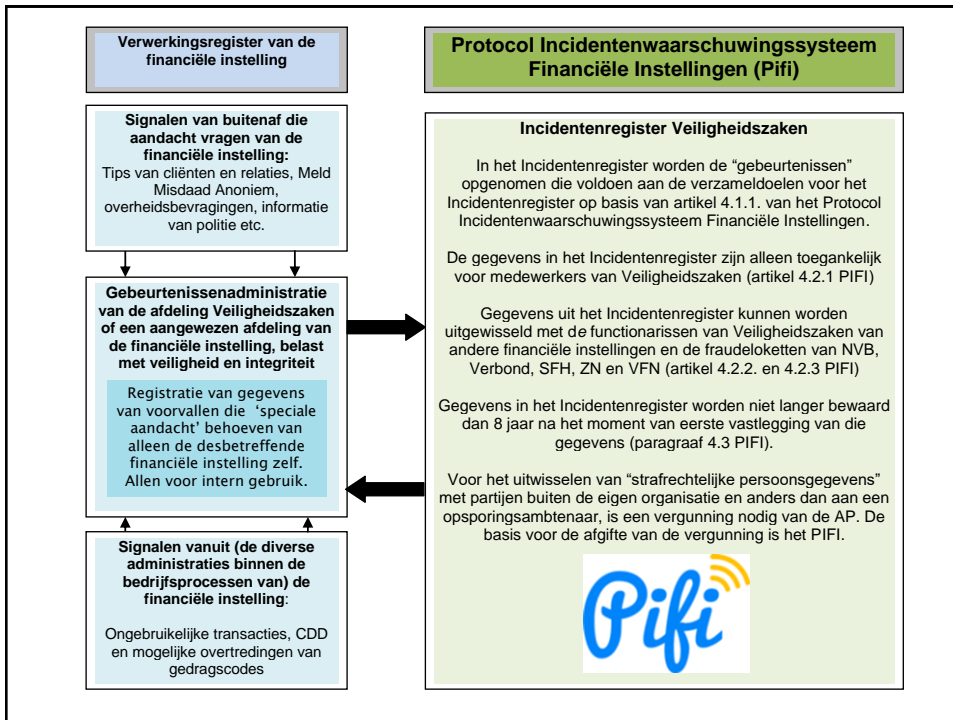
FIM (Rabobank)

Wat betekent het wettelijke kader?

Op elk moment moet duidelijk zijn of persoonsgegevens onder de Gebeurtenissenadministratie, het Incidentenregister of zowel onder GA & IR vallen.

Uiterlijk op het moment van het delen van strafrechtelijke persoonsgegevens met een derde partij moet Veiligheidszaken van de financiële instelling het incident in het incidentenregister hebben opgenomen.





AVG en fraudeonderzoek

- Verschillende fasen in het onderzoek
- Wat is de aard van de gegevens die verwerkt worden?
- Wat is de relatie tussen AVG en Pifi?
- Vastlegging en verantwoording, het nieuwe mantra



Vijf fasen in het onderzoek



Fraudeonderzoek en AVG (1)

Van ieder onderzoek (CDD of fraude) worden persoonsgegevens vastgelegd in de onderzoeksadministratie (dossiers).

Er is immers sprake van een geheel of gedeeltelijke geautomatiseerde vastlegging van persoonsgegevens.



Fraudeonderzoek en AVG (2)

Kenmerkend voor fraudedossiers is dat persoonsgegevens “van strafrechtelijke aard” worden verwerkt.

Er geldt een verbod tot verwerking van “strafrechtelijke persoonsgegevens”, tenzij de Uitvoeringswet AVG (UAVG) dat toestaat.



Fraudeonderzoek en AVG (3)

Wat zijn “strafrechtelijke persoonsgegevens”?

1. Er zijn concrete aanwijzingen (“min of meer gegronde bedenkingen”) zijn dat een bepaalde persoon strafbaar (heeft) (ge)handel(d)t. **(ruime definitie)**
2. Na het onderzoek en de waardering van het bewijsmateriaal staat vast dat het strafbare feit door een bepaalde persoon (geïdentificeerd) is begaan. De Hoge Raad:

“Er zodanige concrete feiten en omstandigheden dat zij een als strafbaar feit te kwalificeren bewezenverklaring - in de zin van artikel 350 van het Wetboek van strafvordering - kunnen dragen.”
(enge definitie)

Fraudeonderzoek en AVG (4)

Zoals gezegd: Er geldt een verbod tot verwerking van “strafrechtelijke persoonsgegevens”, tenzij de Uitvoeringswet AVG (UAVG) dat toestaat.

UAVG: Ondernemingen mogen strafrechtelijke gegevens verwerken:

- "ten eigen behoefte": Obvion of DLL
- binnen een groep : **Coöperatieve Rabobank U.A**
- "voor derden" onder voorwaarden: **branche**



Uitzonderingen in de AVG (1)

1. Bedrijven en instellingen mogen strafrechtelijke persoonsgegevens voor zichzelf verwerken (art. 33 lid 2 UAVG) (“ten eigen behoefte”).
2. Strafrechtelijk gegevens mogen “voor derden” worden verwerkt, indien deze derde een rechtspersoon is die in dezelfde groep is verbonden als bedoeld in artikel 24b van Boek 2 van het Burgerlijk Wetboek (art. 33 lid 4 onder b UAVG) (concernverbanden).



Uitzonderingen in de AVG (2)

3. Strafrechtelijke gegevens mogen “voor derden” worden verwerkt door verwerkingsverantwoordelijken die optreden krachtens een vergunning op grond van de Wet particuliere beveiligingsorganisaties en recherchebureaus (Wpbr) (art. 33 lid 4 onder b UAVG);



Uitzonderingen in de AVG (3)

4. Uitwisseling strafrechtelijke gegevens met derden in andere situaties?

FRAUDE



Fraudehulpdesk mag geen strafrechtelijke gegevens verwerken

2 november 2021

De Fraudehulpdesk mag geen gegevens over mogelijke daders van fraude verzamelen en bewaren. De Autoriteit Persoonsgegevens (AP) heeft een vergunningsaanvraag hiervoor deze zomer afgewezen. De Fraudehulpdesk is geen opsporingsinstantie en heeft die strafrechtelijke gegevens niet nodig voor zijn taak. Bovendien zouden mensen in de systemen van de Fraudehulpdesk niet de rechten hebben die verdachten bij de politie wél hebben. En kunnen mensen onterecht als fraudeur bestempeld worden.

<https://www.securitymanagement.nl/fraudehulpdesk-mag-geen-strafrechtelijke-gegevens-verwerken/>

The screenshot shows the website of the Autoriteit Persoonsgegevens (AP). The main article is titled "AP wijst aanvraag vergunning zwarte lijst VODIOM af" and is dated 21 oktober 2021. The article discusses the AP's decision to reject a permit application from VODIOM to maintain a black list of suspected fraudsters. The text states that VODIOM wants to share personal data of suspected fraudsters across various sectors like the payment industry, online retail, and telecommunications. The AP's decision is based on the fact that VODIOM is not a law enforcement agency and does not have the legal basis to process such data for its purposes.

AP wijst aanvraag vergunning zwarte lijst VODIOM af

Nieuwsbericht / 21 oktober 2021
Categorie: Vergunning aanvragen, Zwarte lijst

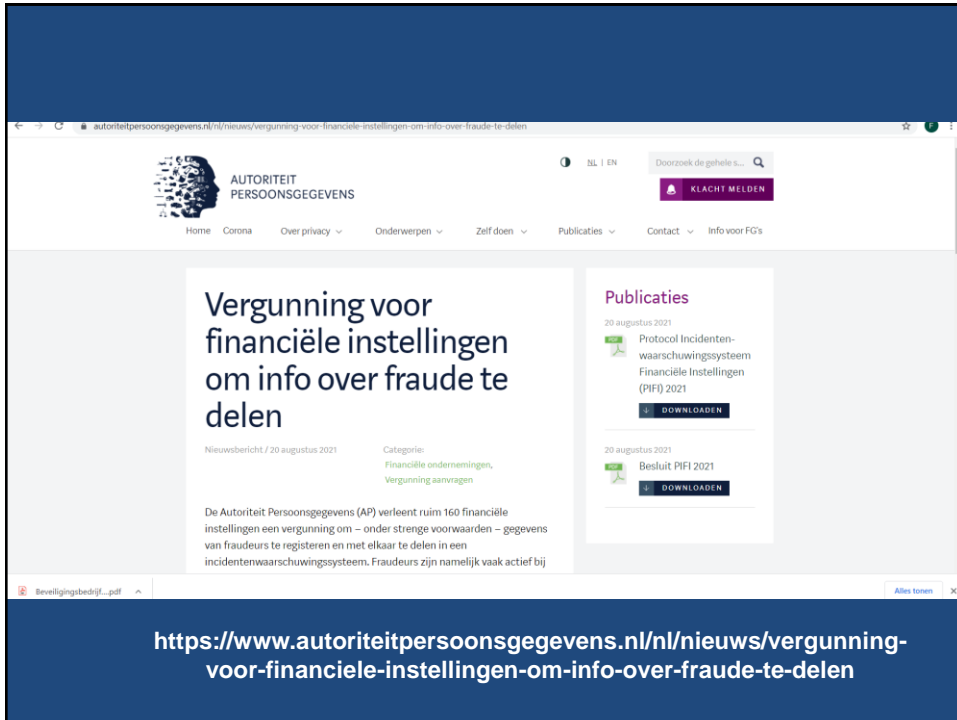
Vereniging VODIOM mag geen zwarte lijst bijhouden van mogelijke fraudeurs, en die zwarte lijst delen met bedrijven uit verschillende sectoren. De Autoriteit Persoonsgegevens (AP) heeft een vergunningsaanvraag hiervoor afgewezen. Mensen die (onterecht) op zo'n zwarte lijst staan, kunnen te maken krijgen met stigmatisering. Private organisaties mogen daarom niet zomaar een 'fraudeursdatabase' beheren en delen.

Vereniging Veilig Ondernemen door Informatie op Maat (VODIOM) is een

Vereniging Veilig Ondernemen door Informatie op Maat (VODIOM) is een initiatief van onder meer belangenorganisatie MKB Nederland.

VODIOM wil persoonsgegevens van vermoedelijke daders van fraude gaan uitwisselen tussen bedrijven in verschillende sectoren: de betaalindustrie, online retail en telecommunicatie.

<https://www.autoriteitpersoonsgegevens.nl/nl/nieuws/ap-wijst-aanvraag-vergunning-zwarte-lijst-vodiom-af>



The screenshot shows the website of the Autoriteit Persoonsgegevens (AP). The main headline is "Vergunning voor financiële instellingen om info over fraude te delen". Below the headline, it states: "De Autoriteit Persoonsgegevens (AP) verleent ruim 160 financiële instellingen een vergunning om – onder strenge voorwaarden – gegevens van fraudeurs te registreren en met elkaar te delen in een incidentenwaarschuwingssysteem. Fraudeurs zijn namelijk vaak actief bij". To the right, there is a "Publicaties" section with two items: "Protocol Incidentenwaarschuwingssysteem Financiële Instellingen (PIFI) 2021" and "Besluit PIFI 2021", both with "DOWNLOADEN" buttons.

<https://www.autoriteitpersoonsgegevens.nl/nl/nieuws/vergunning-voor-financiele-instellingen-om-info-over-fraude-te-delen>

Uitzonderingen in de AVG (3)

4. Uitwisseling strafrechtelijke gegevens met derden in andere situaties?

met een vergunning van de AP
(art. 33 lid 4 onder c en lid 5 UAVG)



Branchewaarschuwinglijsten

Wat is het Pifi?

Pifi is de afkorting voor Protocol Incidenten-waarschuwingstelsysteem financiële instellingen.

Het Pifi bestaat uit een stelsel van afspraken over de uitwisseling van persoonsgegevens binnen de financiële sector, tussen expliciet in het Pifi aangewezen partijen.

Het Pifi is geschreven tegen de achtergrond dat financiële instellingen samen wensen te werken op het gebied van het beheersen van fraude, veiligheid en integriteit.

**WAT DOEN WE
MET DE
CONCURRENTIESTRIJD**

**ALS BLIJKT DAT
WE ALLEMAAL
UNIEK ZIJN**

Loesje

POSTBUS 4801 1000 CA AANHEM

**WAAROM
MOEILIK DOEN
ALS
HET SAMEN KAN**

Loesje

Wie zijn betrokken bij het Pifi?

Dat zijn de vijf brancheverenigingen van de financiële sector. Zij onderhouden het Pifi, coördineren de toelating van deelnemers aan de gegevensuitwisseling en monitoren de naleving van het Pifi door hun leden.

En daarnaast kennen we deelnemers. Dat zijn financiële instellingen, zoals een bank en/of verzekeraar en/of hypothecaire instelling en/of financieringsonderneming.

De deelnemers zijn zelf verantwoordelijk voor de persoonsgegevens die zij verwerken worden en voor beslissingen over het uitwisselen van persoonsgegevens.

Uitgangspunten PIFI (1)

Uitwisseling van strafrechtelijke persoonsgegevens is onvermijdelijk. Daarvoor heeft de AP een vergunning verstrekt.

Het PIFI beschrijft een gesloten uitwisselingsysteem op basis van noodzaak en reciprociteit.

Het systeem is alleen toegankelijk voor financiële instellingen met een vergunning van een financieel toezichthouder;

Het is in Europa een uniek systeem.



Uitgangspunten PIFI (2)

De financiële instellingen moeten – in principe - zijn aangesloten bij één van de vijf brancheverenigingen;

De financiële instellingen (“deelnemers”) moeten beschikken over een interne afdeling veiligheidszaken;

Alleen aangewezen medewerkers van veiligheidszaken mogen gegevens uitwisselen uit het incidentenregister;

Het systeem is territoriaal beperkt tot Nederland.



Wat betekent samenwerking?

Samenwerking betekent dat gegevens moeten worden uitgewisseld, indien dat noodzakelijk om de schadelast als gevolg van fraude te beheersen.

Er wordt samengewerkt bij veiligheidskwesties

Zoals:

- Ontslagen personeel dat elders emplooi wil vinden
- Frauderende klanten en ongewenste gasten

Het Pifi regelt twee vormen van samenwerking

1. Het uitwisselen van persoonsgegevens bij het onderzoeken van fraude en criminaliteit (incidenten)

Er worden al dan niet strafrechtelijke persoonsgegevens uitgewisseld met veiligheidszaken van een andere deelnemer, een derde-organisatie als bedoeld in het Pifi of met het fraudeloket van de branchevereniging.

Het Pifi regelt twee vormen van samenwerking

2. Waarschuwingsfunctie door registratie van plegers van incidenten

Deelnemers leggen persoonsgegevens vast van iemand die zich schuldig heeft gemaakt aan sector gerelateerde fraude of criminaliteit, volgens de in het Pifi benoemde opnamecriteria.

Op deze persoon betrekking hebbende gegevens over het incident worden na een hit in het externe verwijzingsregister (EVR) uitgewisseld met veiligheidszaken van de toetser.

Met de verstrekte informatie kan de andere financiële instelling geïnformeerd besluiten of deze persoon een risico vormt voor dienstverlening of indienstneming.

Het Pifi wordt ook door de rechter toegepast

Het Gerechtshof te Amsterdam heeft op 18 januari 2007 beschikt dat het Protocol incidentenwaarschuwingssysteem financiële instellingen als toetsingskader moet worden gehanteerd bij de rechterlijke beoordeling van de AVG.

Citaat: “Het protocol valt te beschouwen als een regeling die voldoende waarborgen biedt voor een verwerking van persoonsgegevens zoals de AVG die voorschrijft”.

Conclusie: Dat betekent dat de rechter in voorkomende gevallen moet toetsen of de financiële instelling het protocol juist heeft toegepast.

Jurisprudentie opname in EVR (1)

Het Gerechtshof Amsterdam stelde op 12 januari 2006 dat opname in het incidentenregister en met name in het daaraan gekoppelde externe verwijzingsregister (EVR) verstreckende gevolgen voor iemand kan hebben.

Gelet daarop dienen hoge eisen te worden gesteld aan de gronden voor opname van iemand in het EVR.

Het is aan de financiële instelling om terzake van het verwijt van frauduleus handelen met specifieke stellingen te komen en van die stellingen bewijs bij te brengen dat voldoende sterk is om opname in het incidentenregister, met alle daaraan verbonden gevolgen te rechtvaardigen.

Jurisprudentie opname in EVR (2)

Het Gerechtshof Amsterdam stelde op 29 november 2007 dat een redelijk vermoeden van schuld van een strafbaar feit zoals dat kan blijken uit een aangifte is onvoldoende.

Zij stelde ook dat voor opname in een waarschuwingsregister **geen strafrechtelijke veroordeling vereist** is. Dat ligt immers niet binnen de invloedssfeer van de instelling die deelneemt aan het systeem.

Wel moeten de feiten en de betrokkenheid bij de misdraging in voldoende mate vaststaan.

De Hoge Raad heeft deze uitgangspunten bevestigd.

Jurisprudentie opname in EVR (3)

De jurisprudentie van lagere rechters laat zien dat de rechter aan de hand van de overlegde stukken in het geding heel feitelijk toetst of voldaan wordt aan de opnamecriteria voor EVR.

Dossiers bieden vaak onvoldoende houvast voor vaststelling van daadwerkelijke betrokkenheid van de geregistreeerde bij de verweten gedraging.

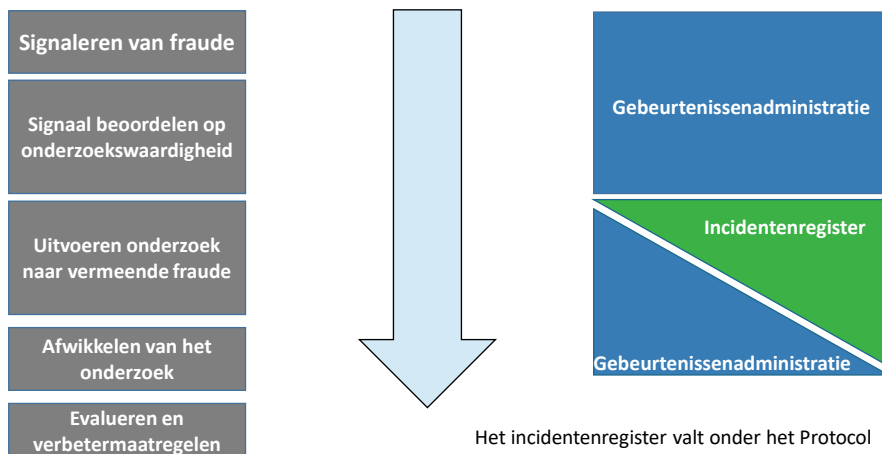
Praktijkcase aan de hand van het 5 fasen model

5-Fasen model van onderzoek

1. signaleren van mogelijke fraude
2. fraudesignaal beoordelen op onderzoekswaardigheid
3. uitvoeren van het onderzoek
4. afwickelen van het onderzoek
5. evaluatie



De Juridische status van de vastlegging van persoonsgegevens kan wijzigen naarmate het onderzoek in een andere fase zit.



Het incidentenregister valt onder het Protocol Incidentenwaarschuwingssysteem financiële instellingen (Pifi)

Fase 1: signaleren

Wat is de aanleiding voor jouw onderzoek?



Casus fraude door klant (kredietfraude)

Klant vraagt een consumptief krediet van € 20.000.- aan bij een lid van de VFN (bijvoorbeeld Santander).

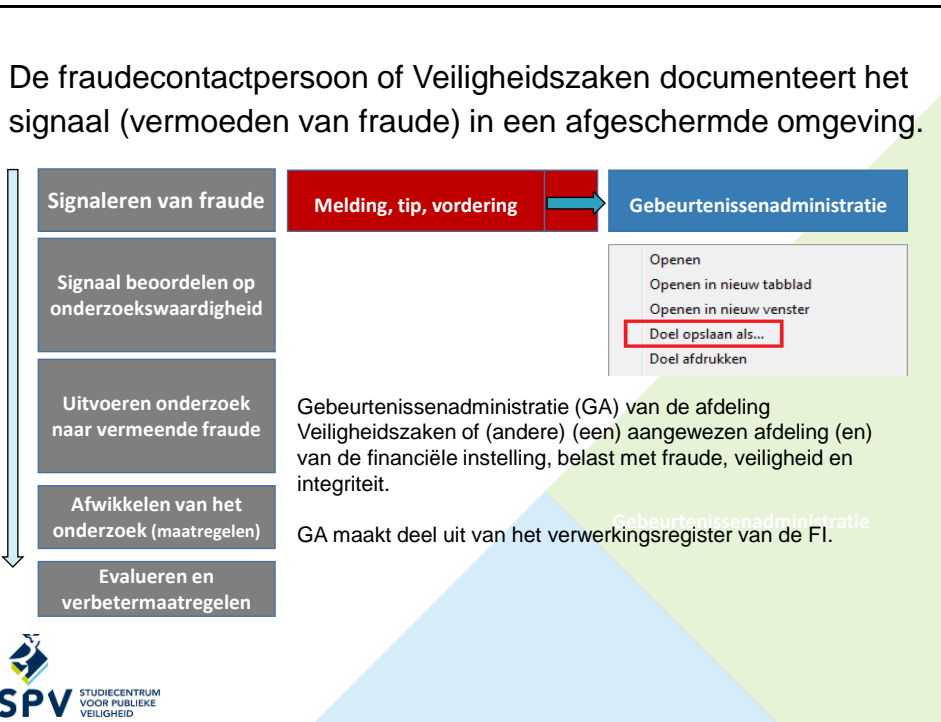


Om de kredietverlener te overtuigen dat hij over voldoende en reguliere inkomsten beschikt, maakt hij een valse werkgeversverklaring en valse loonstroken. Deze overlegt hij aan Santander.



De medewerker van de frontoffice van Santander vertrouwt het niet en meldt het vermoeden van fraude bij de fraudecontactpersoon van de afdeling of rechtstreeks bij Veiligheidszaken en onderbouwt het vermoeden met argumenten.

In welke "onderzoeksalministratie" legt Santander dit signaal vast?



Vervolg onderzoek kredietaanvraag

Uitgangspunt voor kredietverstrekking:



Het is – mede – ter voorkoming van overkreditering van essentieel belang dat de kredietgever volledig kan vertrouwen op de juistheid en getrouwheid van de verstrekte gegevens.

Voortzetting van het onderzoek:

Het signaal van mogelijke kredietfraude wordt beoordeeld op onderzoekswaardigheid.

Vervolg van het onderzoek kredietaanvraag

Veiligheidszaken Santander vraagt de stukken op uit hun kredietdossier en analyseert deze. Daarbij valt het volgende op:

- ▶ Het opgegeven salaris van € 73.290 per jaar is relatief hoog voor een 27-jarige.
- ▶ De opgegeven werkgever komt niet voor in de Kvk en heeft geen website.
- ▶ Op de loonstroken kloppen de Inhoudingsbedragen in kolommen normaal tarief, totaal en cumulatief niet.



Het signaal van mogelijke kredietfraude wordt beoordeeld op onderzoekswaardigheid (door fraudecontactpersoon of VZ).



Fase 3: Uitvoeren onderzoek

Op efficiënte en effectieve wijze onderzoeken of en zo ja, op welke wijze fraude is gepleegd. Daarbij wordt gebruik gemaakt van de 7 W's.



Vervolg van het onderzoek kredietaanvraag

Klant heeft een bankrekening bij ING.

VZ Santander is voornemens om VZ van ING te benaderen voor informatie.

VZ Santander wil graag weten of sprake is van maandelijkse salarisoverboekingen door de werkgever op basis van de arbeidsovereenkomst en de daaruit voortvloeiende en door de klant overlegde loonstroken.

ING 



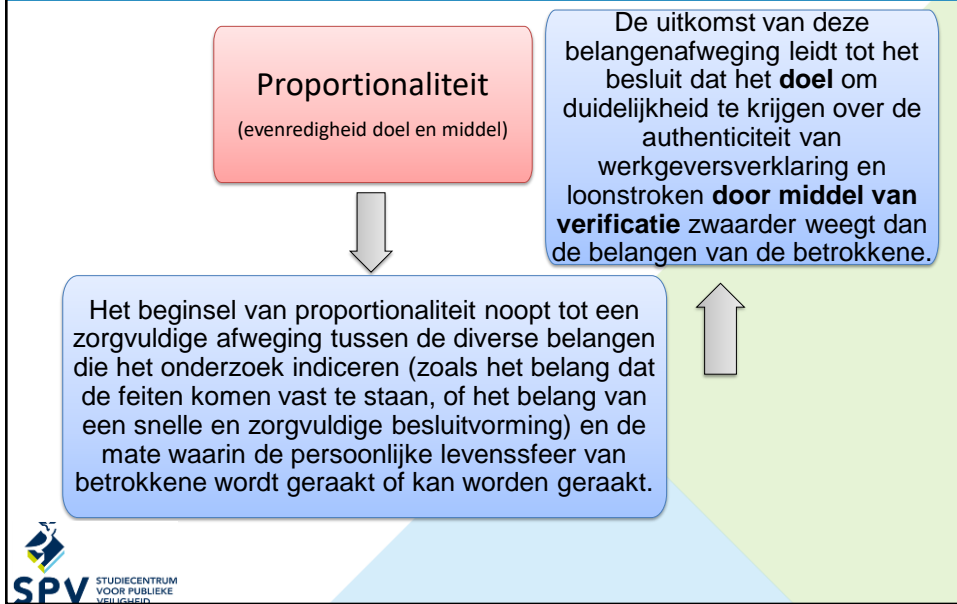
Drie vragen

Waarom heeft Santander niet eerst hun klant om opheldering gevraagd over haar bedenkingen over het dagafschrift voordat zij ING benaderde?

Voordat VZ Santander vragen stelt aan VZ van ING moet VZ van Santander een afweging van belangen maken op basis van art. 6 lid 1 onder f AVG.

De verwerkingsgrondslag van art. 6 lid 1 AVG vergt een afweging van proportionaliteit en subsidiariteit

Verwerkingsgrondslag AVG (6 lid 1 f)



Toegepast op de casus



Hoe doe je dat?

Subsidiariteit



Het beginsel van subsidiariteit stelt de onderzoeker voor de vraag hoe de benodigde informatie kan worden verkregen, op een zodanige wijze dat een zo min mogelijke inbreuk op de persoonlijke levenssfeer van de klant wordt gemaakt, terwijl de uitkomst van de wijze van vergaren feitelijk tot hetzelfde resultaat leidt.

Verwerkingsgrondslag toegepast

Subsidiariteitsafweging



Het bevragen van een andere instantie (een werkgever of de bank) over de klant, kan vragen oproepen over de betrouwbaarheid van die klant bij die instantie, waardoor deze in de toekomst door de bevroegde instantie aangemerkt wordt als iemand (werknemer of klant) met een verhoogd risico.

Waarom zou de klant vertellen dat de stukken vervalst zijn in de wetenschap dat hij dan kan fluiten naar zijn geld?

Uitwisseling van klantgegevens tussen financiële instellingen vindt alleen plaats tussen veiligheidsafdelingen. Er komt geen aantekening in de klantenadministratie van de bevroegde instelling.

De uitkomst van deze afweging leidt tot het besluit dat bij de andere financiële instelling zal worden geverifieerd of de gegevens en bescheiden kloppen

Drie vragen

Vraag 2

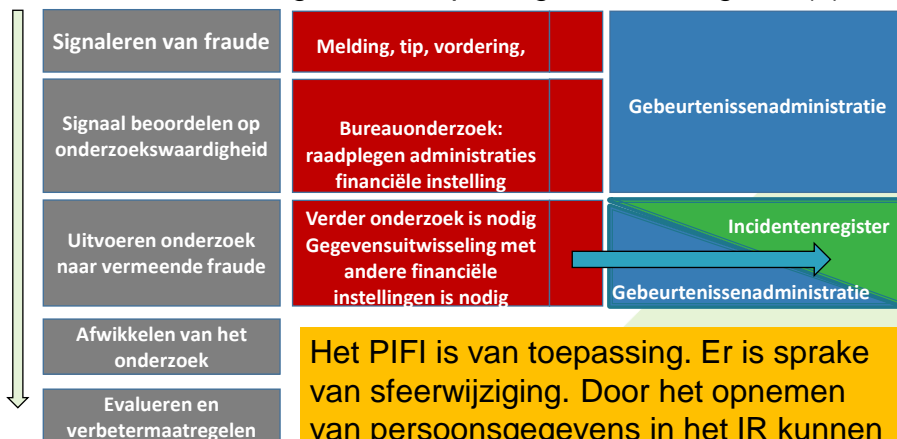
Wat betekent het bevragen van ING door Santander voor de juridische status van de gegevens?

Anders geformuleerd:

Wijzigt er iets in het documenteren van het vermoeden van de fraude door VZ van Santander in hun onderzoeksadministratie?



Vergaren en analyseren en vastleggen van persoonsgegevens die betrekking hebben op veiligheid en integriteit (3)



Vastlegging gegevens in Incidentenregister

Het voornemen van Santander betekent dat gegevens van het onderzoek gedeeld moeten worden met ING.

Er is sprake van sfeerwijziging. Naast opname van het incident in de Gebeurtenissenadministratie wordt de zaak ook opgenomen in het incidentenregister van Santander.

Aan de opnamecriteria van art. 4.1.1. PIFI wordt voldaan.

Persoonsgegevens in het IR kunnen worden gedeeld met de partijen die in het PIFI benoemd worden.

Protocol Incidentenwaarschuwingssysteem Financiële Instellingen (PIFI)

Incidentenregister Veiligheidszaken

In het Incidentenregister worden gegevens vastgelegd van (mogelijke) Incidenten.

Een incident is een gebeurtenis die als gevolg heeft, zou kunnen hebben of heeft gehad dat de belangen, integriteit of veiligheid van de cliënten of medewerkers van een financiële instelling, de financiële instelling zelf of de financiële sector als geheel in het geding zijn of kunnen zijn.

Voor opname van gegevens moet worden voldaan aan de verzameldoelen voor het Incidentenregister die genoemd zijn in artikel 4.1.1. van het Pifi.

De gegevens in het Incidentenregister zijn alleen toegankelijk voor medewerkers van Veiligheidszaken

Gegevens uit het Incidentenregister kunnen worden uitgewisseld met de functionarissen van Veiligheidszaken van andere financiële instellingen en de fraudeloketten van NVB, Verbond, SFH, ZN en VFN (artikel 4.2.2. en 4.2.3 PIFI)

Gegevens in het Incidentenregister worden niet langer bewaard dan 8 jaar na het moment van eerste vastlegging van die gegevens (paragraaf 4.3 PIFI).

Vergaren en analyseren en vastleggen van persoonsgegevens die betrekking hebben op veiligheid en integriteit (4)



Drie vragen

Vraag 3

Mag ING transactiegegevens van de klant uit haar klantenadministratie verstrekken aan Santander?

Voor de beantwoording van die vraag zijn het verwerkingsregister ex art. 30 AVG van ING van belang en hun interne instructies.

Het privacystatement op de ING-website is een afgeleide van het verwerkingsregister en geeft aanknopingspunten voor het antwoord.



Terug naar de algemene beginselen

Doelbepaling en
doelbinding
Art. 5 lid 1 onder b

Persoonsgegevens mogen alleen voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld en mogen niet op een met die doeleinden onverenigbare wijze worden verwerkt.

Waarom verzamelt ING klantgegevens? (1)

← → C ING BANK N.V. [NL] | https://www.ing.nl/de-ing/privacy-statement/wat-doen-we-met-persoonsgegevens/index.html ☆ 0 E

> De ING > Privacy Statement > Wat doen we met persoonsgegevens?

Privacy Statement

- > Goed nieuws voor uw privacy
- > Doel van dit Privacy Statement
- > Welke persoonsgegevens verwerken we?
- > Wat doen we met persoonsgegevens?
- > Met wie delen we gegevens en waarom?
- > Gebruik maken van uw rechten (Nederland)
- > Uw verplichting om gegevens te verstrekken
- > Hoe beschermen we uw persoonsgegevens?
- > Wat kunt u doen om uw gegevens te beschermen?
- > Hoe lang bewaren we persoonsgegevens?
- > Contact en vragen over

Wat doen we met persoonsgegevens?

We gebruiken uw persoonsgegevens alleen op basis van de volgende wettelijke grondslagen:

- om een contract met u te sluiten en uit te voeren;
- om te voldoen aan wettelijke verplichtingen;
- voor ons 'gerechtvaardigd bedrijfsbelang'. Hierbij verwerken we gegevens om goede commerciële banden met al onze klanten en andere betrokken partijen te onderhouden, om fraude te voorkomen en te bestrijden en de veiligheid van uw transacties en onze bedrijfsvoering te bewaken;
- op basis van uw toestemming. Deze toestemming kunt u altijd weer intrekken.

We kunnen uw gegevens voor de volgende doelen verwerken:

▼ Administratie
▼ Levering van producten en diensten
▼ Beheer van klantrelaties
▼ Analyse van kredietrisico en gedrag

Waarom verzamelt ING klantgegevens? (2)

← → C ING BANK N.V. [NL] | https://www.ing.nl/de-ing/privacy-statement/wat-doen-we-met-persoonsgegevens/index.html ☆ 0 E

- > Uw verplichting om gegevens te verstrekken
- > Hoe beschermen we uw persoonsgegevens?
- > Wat kunt u doen om uw gegevens te beschermen?
- > Hoe lang bewaren we persoonsgegevens?
- > Contact en vragen over privacy (Nederland)
- > Over dit Privacy Statement

op basis van uw toestemming. Deze toestemming kunt u altijd weer intrekken.

We kunnen uw gegevens voor de volgende doelen verwerken:

▼ Administratie
▼ Levering van producten en diensten
▼ Beheer van klantrelaties
▼ Analyse van kredietrisico en gedrag
▼ Persoonlijke marketing op basis van profilering
▼ Aanbieden van passende producten en diensten
▼ Verbetering en ontwikkeling van producten en diensten
▲ Voorkomen en herkennen van fraude en gegevensbeveiliging

We hebben de plicht om uw persoonsgegevens te beschermen en inbreuken op de beveiliging ervan te voorkomen, detecteren en beperken. Dit geldt ook voor de informatie die wij verplicht over u moeten verzamelen. Bijvoorbeeld om te voldoen aan de wet- en regelgeving tegen witwassen, financiering van terrorisme en belastingfraude.

- We kunnen uw persoonsgegevens verwerken met als doel u en uw financiële bezittingen te beschermen tegen frauduleuze activiteiten, bijvoorbeeld als u slachtoffer bent geworden van

Met wie deelt ING klantgegevens? (1)

← → C ING BANK N.V. [NL] | https://www.ing.nl/de-ing/privacy-statement/met-wie-delen-we-gegevens-en-waarom/index.html

Particulier Personal Banking Private Banking Zakelijk > Hulp bij inloggen **Inloggen**

ING Home Service & Contact Zoeken

> De ING > Privacy Statement > Met wie delen we gegevens en waarom?

Privacy Statement

- > Goed nieuws voor uw privacy
- > Doel van dit Privacy Statement
- > Welke persoonsgegevens verwerken we?
- > Wat doen we met persoonsgegevens?
- > Met wie delen we gegevens en waarom?
- > Gebruik maken van uw rechten (Nederland)
- > Uw verplichting om gegevens te verstrekken
- > Hoe beschermen we uw persoonsgegevens?
- > Wat kunt u doen om uw

Met wie delen we gegevens en waarom?

Om u de best mogelijke diensten te kunnen verlenen en concurrerend te blijven, delen we bepaalde gegevens binnen en buiten ING. Daarbij gaat het om:

- ▼ ING-onderdelen
- ▼ Tussenpersonen
- ▼ Overheidsinstanties
- ▼ Financiële instellingen
- ▼ Dienstverleners die voor ING werken
- ▼ Onderzoekers
- ▼ Bedrijven waar we mee samen werken (Nederland)
- ▼ Met andere bedrijven: als u daarom vraagt (Nederland)

Met wie deelt ING klantgegevens? (2)

← → C ING BANK N.V. [NL] | https://www.ing.nl/de-ing/privacy-statement/met-wie-delen-we-gegevens-en-waarom/index.html

Particulier Personal Banking Private Banking Zakelijk > Hulp bij inloggen **Inloggen**

ING Home Service & Contact Zoeken

> De ING > Privacy Statement > Met wie delen we gegevens en waarom?

Privacy Statement

- > Goed nieuws voor uw privacy
- > Doel van dit Privacy Statement
- > Welke persoonsgegevens verwerken we?
- > Wat doen we met persoonsgegevens?
- > Met wie delen we gegevens en waarom?
- > Gebruik maken van uw rechten (Nederland)
- > Uw verplichting om gegevens te verstrekken
- > Hoe beschermen we uw persoonsgegevens?
- > Wat kunt u doen om uw gegevens te beschermen?
- > Hoe lang bewaren we persoonsgegevens?
- > Contact en vragen over

Met wie delen we gegevens en waarom?

Om u de best mogelijke diensten te kunnen verlenen en concurrerend te blijven, delen we bepaalde gegevens binnen en buiten ING. Daarbij gaat het om:

- ▼ ING-onderdelen
- ▼ Tussenpersonen
- ▼ Overheidsinstanties
- ▲ Financiële instellingen

Onze afdeling Veiligheidszaken kan persoonsgegevens delen met de afdeling Veiligheidszaken van andere financiële instellingen.

Waarborg ter voorkoming van stigmatisering van betrokkene: Uitwisseling van gegevens vindt alleen plaats tussen geautoriseerde medewerkers van Veiligheidszaken.

Nederlandse Vereniging van Banken (NVB).

Mag ING gegevens vertrekken?

Santander legt uit dat het noodzakelijk is om gegevens van ING te krijgen vanwege het concrete vermoeden van fraude.

Er is geen sprake van een gezamenlijk onderzoek. ING heeft zelf geen incident. Toch is gegevensverstrekking mogelijk.

Het Pifi is niet van toepassing op een Eventuele verstrekking door ING.

ING moet belangen afwegen:



Hoe verhoudt zich het raadplegen van de klantenadministratie en het verstrekken van gegevens aan Santander tot de belangen en rechten van de ING-klant? (art. 6 lid 1 onder f AVG).



Op het beantwoorden van de vraag door ING is het PIFI voor ING niet van toepassing. De klantenadministratie wordt geraadpleegd.

Waarom verzamelt ING klantgegevens? En voor wie zijn deze gegevens bestemd? Dit heeft ING vastgelegd in haar verwerkingsregister (ex art. 30 AVG). Een afgeleide daarvan staat in het privacystatement op hun website.

De Verwerking van persoonsgegevens van klanten door ING vindt, plaats in het kader van een efficiënte en effectieve bedrijfsvoering, in het bijzonder gericht op de volgende activiteiten:

- het beoordelen en accepteren van (potentiële) klanten, het aangaan en uitvoeren van overeenkomsten met een betrokkene en het afwikkelen van het betalingsverkeer;
- het verrichten van analyses van persoonsgegevens ten behoeve van statistische en wetenschappelijke doeleinden;
- het uitvoeren van (gerichte) marketingactiviteiten teneinde een relatie met een betrokkene tot stand te brengen en/of met een klant in stand te houden dan wel uit te breiden;
- het waarborgen van de veiligheid en integriteit van de sector, daaronder mede begrepen het bestrijden, voorkomen en opsporen van (pogingen tot) (strafbare) gedragingen gericht tegen de branche waar de bank deel van uitmaakt, de groep waartoe de bank behoort, de bank zelf, haar klanten en medewerkers, alsmede het gebruik van en de deelname aan waarschuwingssystemen;
- het voldoen aan wettelijke verplichtingen.

ING legt de bevraging en het antwoord vast in hun GA



Verantwoordingsplicht (1)



ING 

 Santander

- ▶ De interne afwegingen om te komen tot de verstrekking van gegevens aan veiligheidszaken van een andere financiële instelling,
- ▶ de wijze van bevragen, de wijze waarop wordt geïnformeerd (en als dat niet gebeurt de reden daarvoor) alsmede de proportionaliteits- en subsidiariteitsafwegingen dienen door veiligheidszaken in haar administratie te worden vastgelegd.

Verantwoordingsplicht (2)

- ▶ In de onderzoeksadministratie van Santander moet de toegepaste onderzoeksmethode (verificatievraag of bevraging) worden benoemd onder vermelding van de gronden die tot de toepassing daarvan heeft geleid.
- ▶ Door middel van deze verslaglegging is achteraf toetsing mogelijk op de juiste toepassing van onderzoeksmethoden- en middelen.



Verantwoordingsplicht / Accountability

Verplichting voor organisaties om aan te tonen dat gegevensverwerkingen voldoen aan de AVG

Rechtmatigheid
Transparantie
Doelbinding
Juistheid

 Santander

Registratie IR ongedaan maken

- ▶ Indien onvoldoende kan worden aangetoond dat iemand verwijtbaar betrokken is bij vermeend wangedrag dienen diens persoonsgegevens te worden verwijderd uit het IR.



Het in artikel 4.1.1 PIFI omschreven doel wordt dan immers niet meer met de registratie gediend.



FASE 4 AFWIKKELEN ONDERZOEK

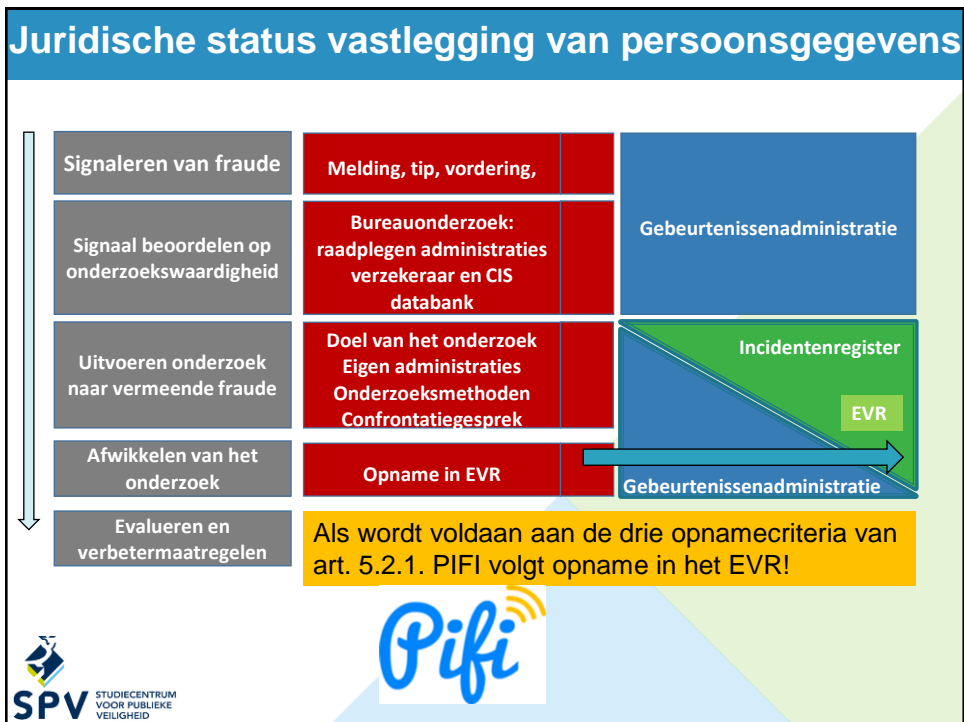
KLANTENSCHERMING

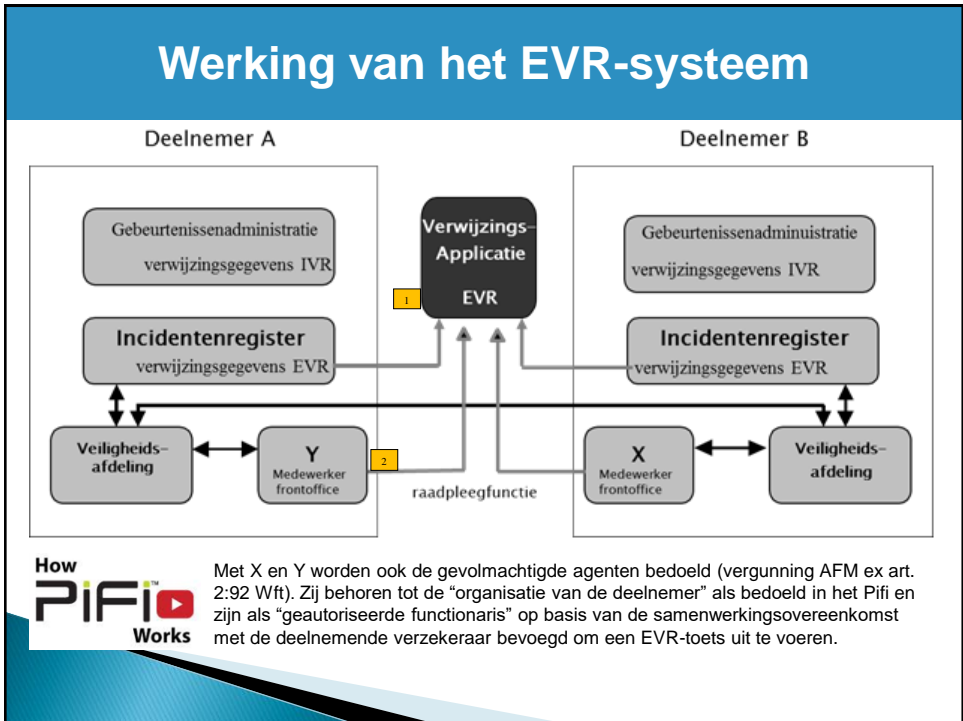
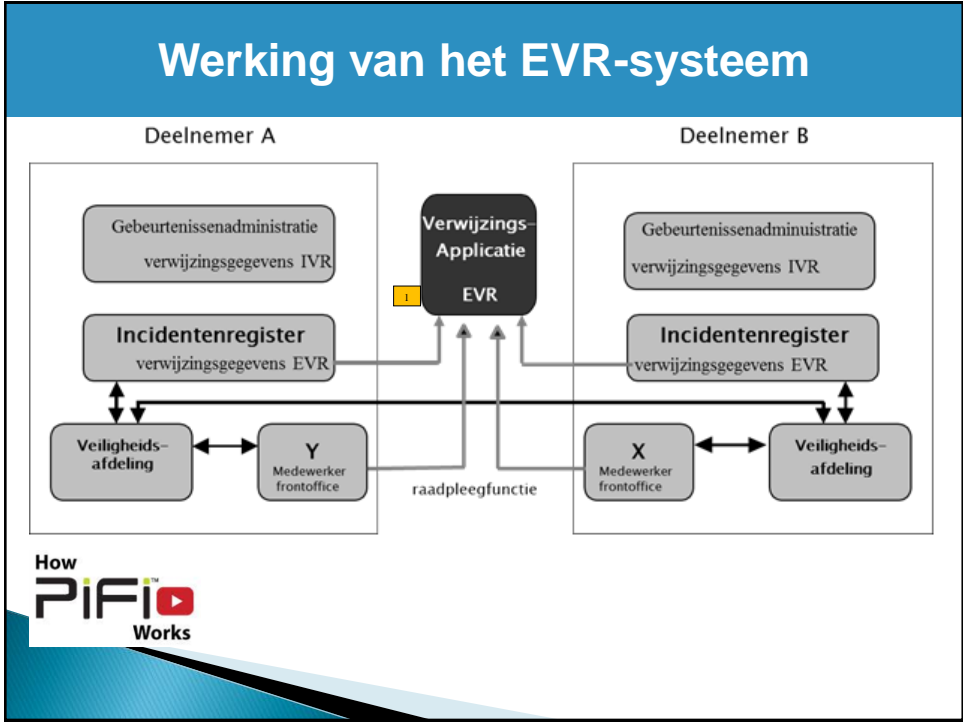
Op de zwarte lijst
van banken: in de
financiële gevangenis

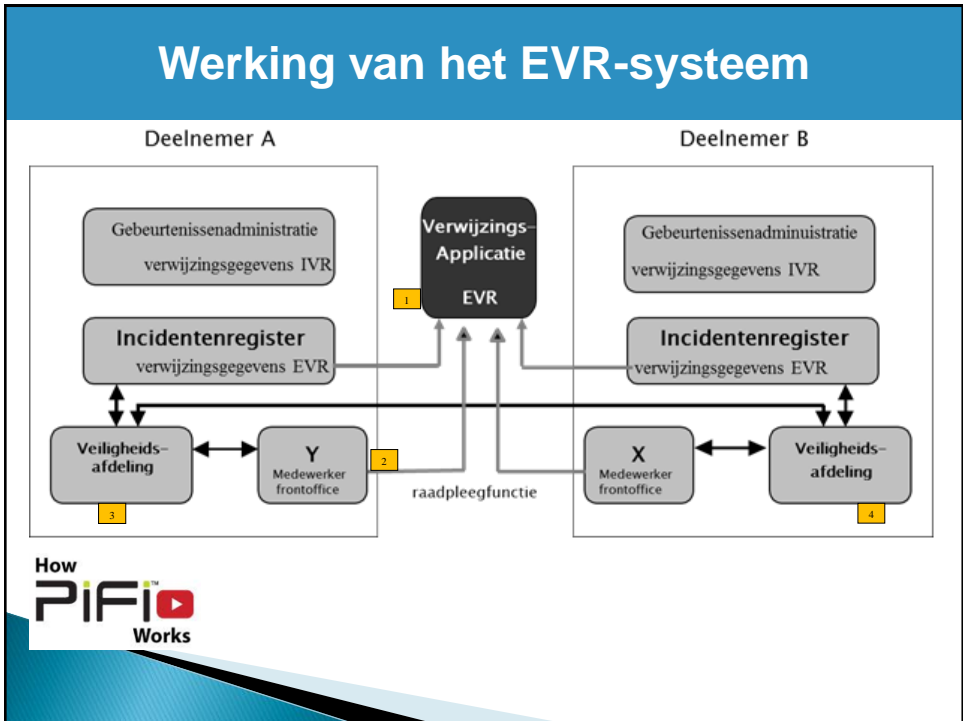
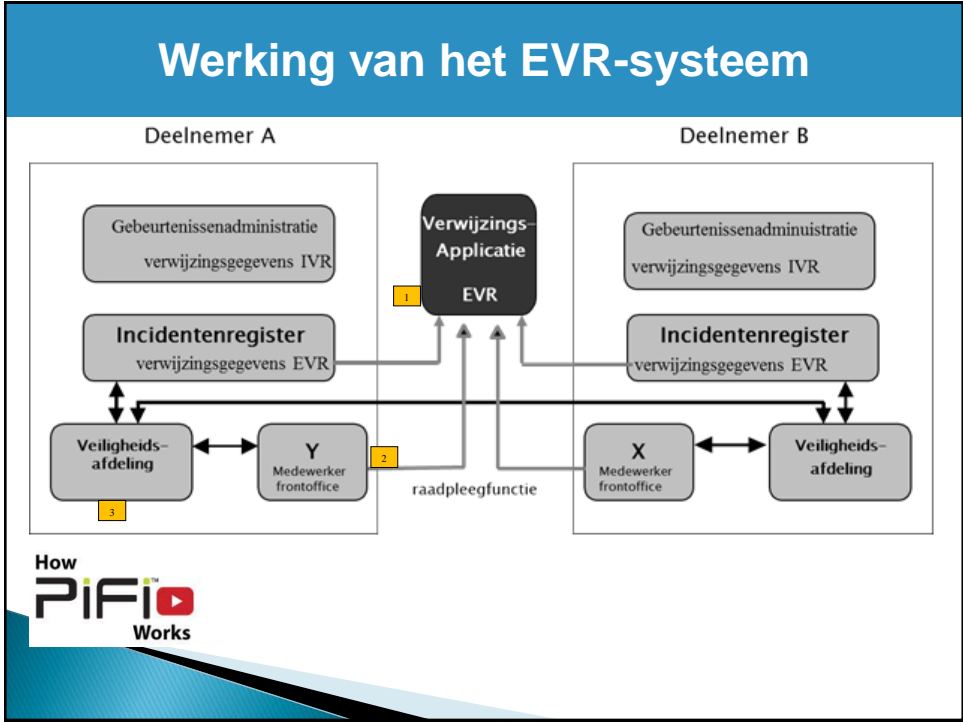
Duizenden Nederlanders zijn door banken op verdenking van fraude op een zwarte lijst geplaatst. Ze krijgen nergens een bankrekening of hypotheek. Zelfs niet als de rechter hen vrijspreekt.

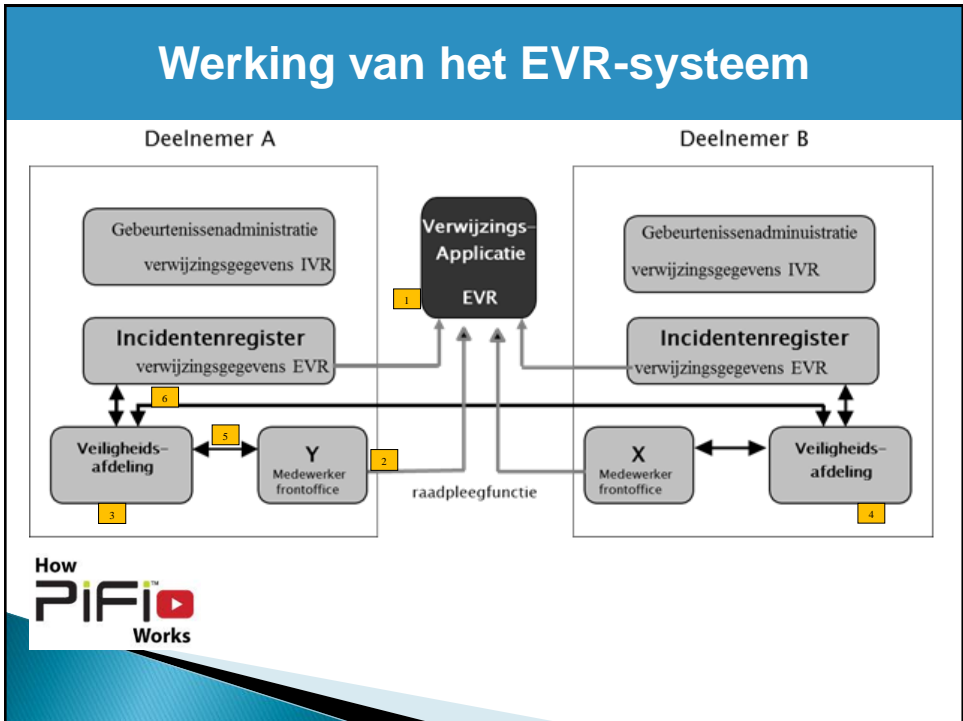
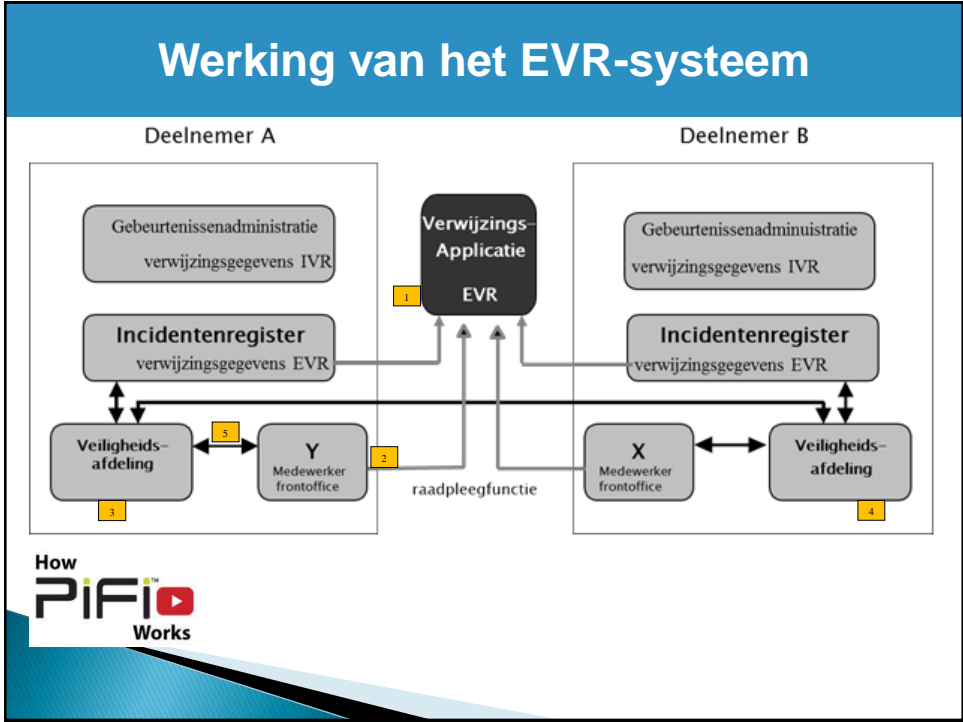
Tekst **Camil Driessen** en **Joris Koolman** Illustratie **Pepijn Barnard**

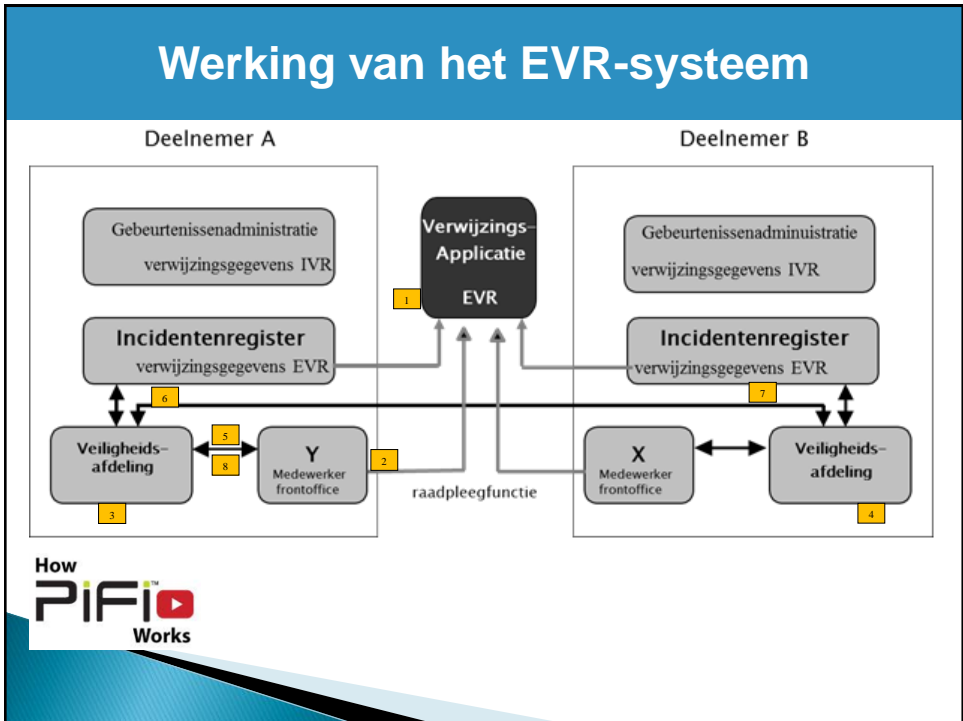
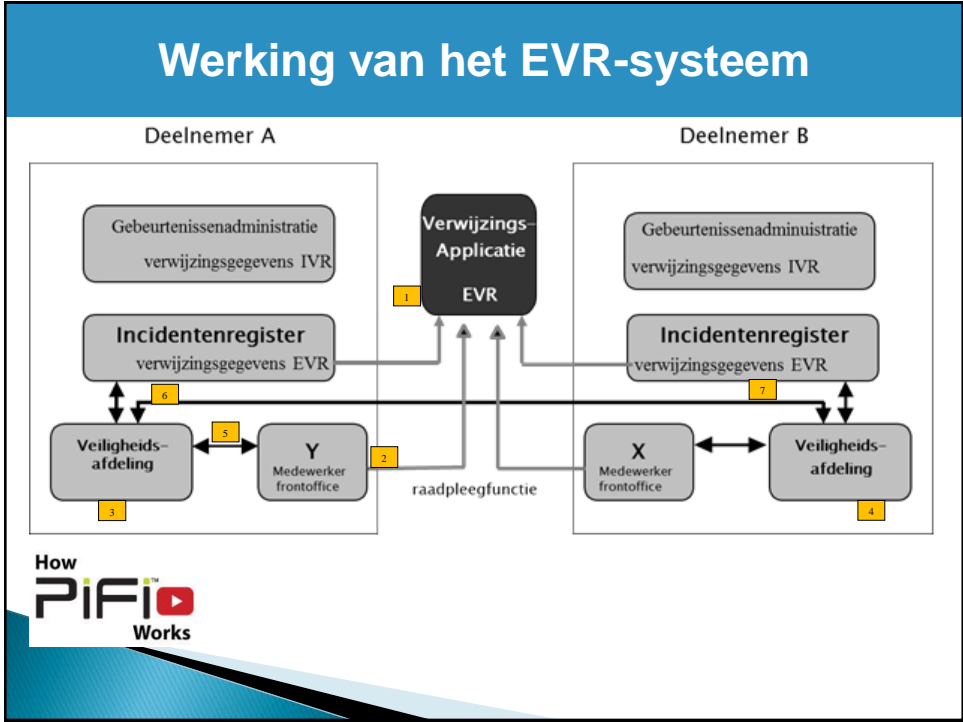


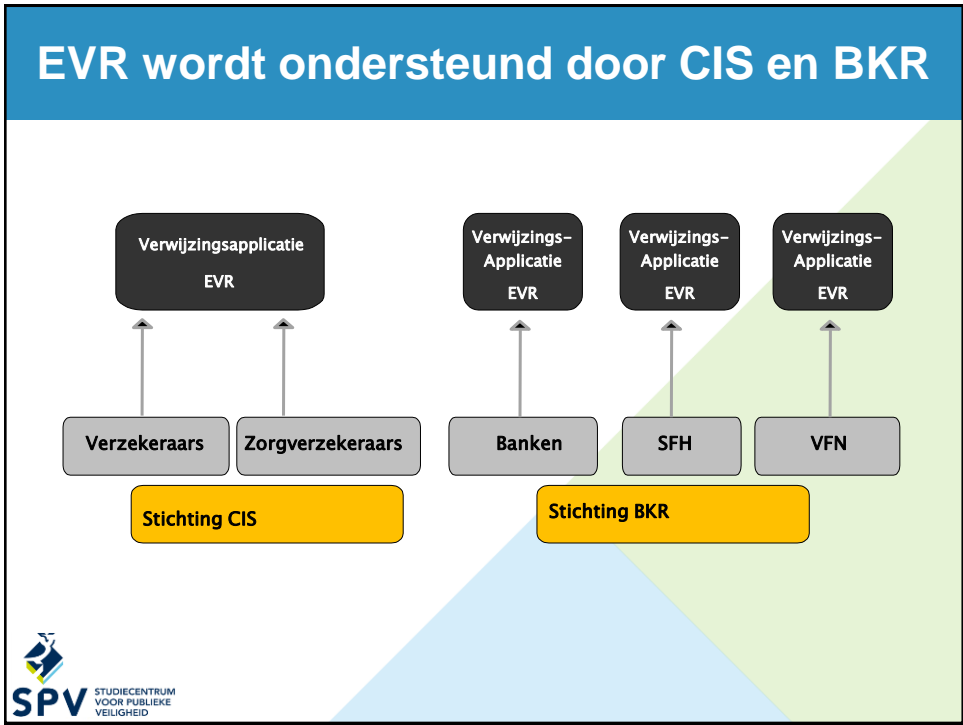
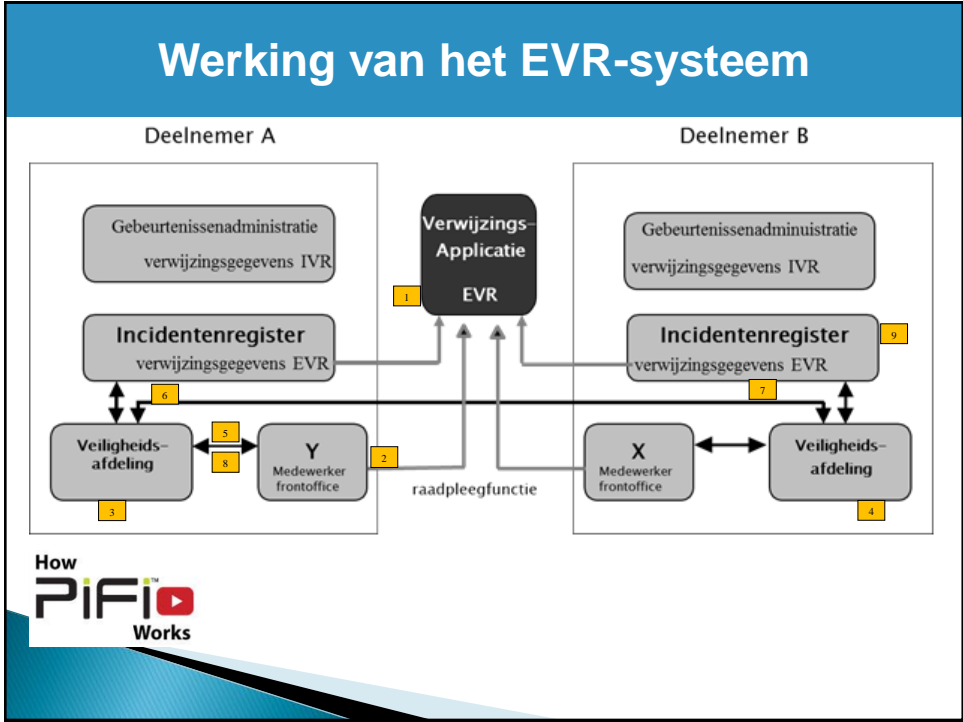








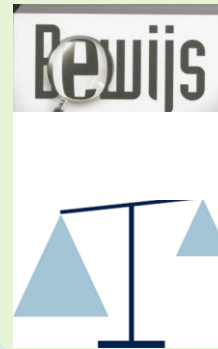




Opnamecriteria voor EVR

Artikel 5.2.1 PIFI

1. Is vastgesteld dat de **gedraging(en)** van de (rechts)persoon een bedreiging vormen, vormen of kunnen vormen?
2. **Staat in voldoende mate staat vast** dat de betreffende (rechts)persoon betrokken is bij de onder 1 bedoelde gedraging(en).
3. Is **het belang van opname zwaar genoeg** in vergelijking met de mogelijk nadelige gevolgen voor betrokkene? (proportionaliteitsafweging)



1e criterium: de gedraging

Gerechtshof 's-Hertogenbosch. 27 augustus 2019, ECLI:NL:GHSHE:2019:3189

“Het hof is van oordeel dat artikel 5.2.1. PIFI met zich brengt dat bij de registratie voor de geregistreerde duidelijk moet zijn welke gedragingen volgens de deelnemer een zodanige bedreiging vormen dat deze registratie rechtvaardigen.

Dit maakt bovendien voor de rechter toetsbaar of de persoonsgegevens van de geregistreerde al dan niet ten onrechte in het EVR zijn opgenomen.”

1e criterium: de gedraging

Gerechtshof 's-Hertogenbosch. 27 augustus 2019, ECLI:NL:GHSHE:2019:3189

“Het hof is van oordeel dat artikel 5.2.1. PIFI met zich brengt dat bij de registratie voor de geregistreerde **duidelijk moet zijn welke gedragingen volgens de deelnemer een zodanige bedreiging vormen dat deze registratie rechtvaardigen.**

Dit maakt bovendien voor de rechter toetsbaar of de persoonsgegevens van de geregistreerde al dan niet ten onrechte in het EVR zijn opgenomen.”

1e criterium: de gedraging

De registraties in EVR hebben doorgaans betrekking op personen die een strafbaar feit hebben gepleegd, waarbij de klant of de financiële instelling benadeeld is.

De registraties in EVR kunnen echter ook betrekking hebben op wanprestatie (bijvoorbeeld het opzettelijk schenden van geldende hypotheekvoorwaarden of polisvoorwaarden).*



225 e/o 326 Sr



Wijzigen v/d
bestemming

*Zie bijvoorbeeld: Rechtbank Middel-Nederland 25 november 2021, ECLI:NL:RBMNE:2021:5837

Formuleer de gedraging Voorbeeld

- ▶ Aan de betrokkene is een hypothecaire geldlening van € 264.000,00 verstrekt voor de aankoop van een woning.
- ▶ In de woning is nadien een hennepkwekerij aangetroffen.
- ▶ Betrokkene is gebonden aan de voor hem geldende hypotheekvoorwaarde, welke hij heeft geschonden:

“Hypotheekgever dient geldgever terstond in kennis te stellen van iedere omstandigheid van feitelijke of juridische aard, waardoor de zekerheidswaarde van het onderpand kan verminderen, of die voor geldgever in verband met haar hypotheekrecht van belang kan zijn”.

Formuleer waarom die gedraging onacceptabel is

- ▶ “Het risico op brand in een woning wanneer zich daarin hennepdrogerijen/kwekerijen bevinden is groter is dan wanneer dergelijke – illegale – activiteiten zich niet in een woning afspelen.
- ▶ Het kan de hypothecair financier schaden omdat – naar de ervaring leert – sprake is van risicoverzwaarig die ten gevolge van polisvoorwaarden van een opstalverzekering bij brand tot verlies van dekking leidt.
- ▶ Dit maakt dat de financiële instelling bij een verhypothecarde woning waarin zich een hennepkwekerij/drogerij bevindt, minder (stellige) zekerheid voor de verstrekte lening kan ontlenen aan het onderpand – via de werking van artikel 3:229 BW, zaaksvervanging – dan in het geval een dergelijke activiteit niet wordt ontplooid.”

* Gerechtshof 's-Hertogenbosch 27 maart
2018: ECLI:NL:GHSHE:2018:1303



Formuleer waarom die gedraging onacceptabel is

- ▶ “Het risico op brand in een woning wanneer zich daarin **hennepdrogerijen/kwekerijen** bevinden is groter is dan wanneer dergelijke - illegale - activiteiten zich niet in een woning afspelen.
- ▶ Het kan de hypothecair financier schaden omdat - naar de ervaring leert - **sprake is van risicoverzaring** die ten gevolge van polisvoorwaarden van een opstalverzekering bij brand tot verlies van dekking leidt.
- ▶ Dit maakt dat de financiële instelling bij een verhypotheceerde woning waarin zich een hennepkwekerij/drogerij bevindt, **minder (stellige) zekerheid voor de verstrekte lening kan ontlenen aan het onderpand** - via de werking van artikel 3:229 BW, zaaksvervanging - dan in het geval een dergelijke activiteit niet wordt ontplooid.”



* Gerechtshof 's-Hertogenbosch 27 maart
2018: ECLI:NL:GHSHE:2018:1303



Waarom is de vastgestelde gedraging uit de casus kredietaanvraag onacceptabel?

- ▶ De aard en de hoogte van het inkomen van de kredietnemer vormen de basis van de kredietverstrekking, aangezien Santander (de kredietgever) daarop zal baseren of en tot welk bedrag Santander krediet zal verlenen.
- ▶ Het is dan ook, mede ter voorkoming van overkreditering, van essentieel belang dat de kredietgever op de juistheid en getrouwheid van de verstrekte inkomensgegevens kan vertrouwen.
- ▶ Daarom is het van belang dat frauduleuze handelingen als de onderhavige, die dit vertrouwen ondergraven, worden geregistreerd, ook vanwege de afschrikwekkende werking die daarvan uitgaat.”



* Naar analogie van Rechtbank Den Haag
20 juli 2016: ECLI:NL:RBDHA:2016:9853



2e criterium: voldoende bewijs

- ▶ Hoge Raad: iemand mag alleen in EVR worden opgenomen als in voldoende mate vaststaat dat hij/zij de verweten gedraging gepleegd heeft.
- ▶ Om “strafrechtelijke gegevens” met derden te kunnen uitwisselen, dient sprake te zijn van zodanige concrete feiten en omstandigheden dat zij een als een strafbaar feit te kwalificeren bewezenverklaring in de zin van artikel 350 WvSv kunnen dragen.

2e criterium art. 5.2.1 Documenteer het bewijs

- ▶ Bij registratie in het EVR moet gedocumenteerd worden wat het bewijs is. Dat betekent dat de financiële instelling het bewijs – bij voorkeur – op een overzichtelijke manier moet uitwerken.
- ▶ Deze opgave van bewijsmiddelen is van belang opdat achteraf toetsbaar is, dat voldaan wordt aan de eis van de Hoge Raad uit 2009.

Alternatieve scenario's onderzocht?

Verzekeringnemer claimt inbraakschade op de inboedelverzekering. Verzekeraar overtuigt de rechter dat de inbraak niet kan hebben plaatsgevonden zoals de verzekeringnemer beweert. Vordering tot uitkering onder de polis wordt afgewezen.

Daarmee is nog niet gezegd dat verzekeringnemer fraude heeft gepleegd, in casu opzettelijke misleiding van ABN AMRO door het insceneren van de inbraak. Het bewijs van de verzekeraar sluit immers niet uit dat de diefstal op andere wijze kan hebben plaatsgevonden.

Rechter* gelastte verwijdering gegevens uit Incidentenregister en EVR (CIS)

* Rechtbank Overijssel, 6 februari 2018, ECLI:NL:RBOVE:2018:945

2e criterium art. 5.2.1 Wel of geen aangifte?

- ▶ Bij opname in EVR moet worden afgewogen óf aangifte wordt gedaan óf niet.
- ▶ Opsporingsbelangen of andere belangen kunnen aanleiding zijn om geen aangifte of klachte te doen.
- ▶ Indien geen aangifte (of klachte) wordt gedaan moet met argumenten in het onderzoeksdossier worden vastgelegd waarom geen aangifte (of klachte) is of wordt gedaan.
- ▶ Van louter civiele kwesties kun je geen aangifte doen, maar kan registratie wel gerechtvaardigd zijn. (denk aan overtreding van de voorwaarden van de overeenkomst) (niet melden verhuur deel van de woning aan criminelen voor hennepkwekerij).

Wat moet er gebeuren na een sepot?

- **De jurisprudentie zegt het volgende:**
 “Vanaf het moment dat de financiële instelling bekend is geworden met de seponering van de strafzaak wegens onvoldoende bewijs (sepot 02 = bewijssepot oftewel technisch sepot), is de registratie *in principe* niet langer meer gerechtvaardigd”.
- Zodra financiële instelling bekend is geworden met dat type sepot moet een heroverweging worden gemaakt.
- **Aandachtspunt:** Hebben de feiten die door het OM zijn gewogen betrekking op dezelfde verdenking, dan de verdenking op basis waarvan de financiële instelling tot registratie is overgegaan?

Voorbeeld uit de jurisprudentie (1)

Volgens de bank heeft betrokkene zich schuldig gemaakt aan schuldwitwassen (artikel 420quater WvSr door zijn bankrekening ter beschikking te stellen voor de gepleegde fraude.

De bank heeft vastgesteld dat een door fraude verkregen totaalbedrag van € 4.468,25 in drie transacties is overgeboekt naar de betaalrekening van de betrokkene en dat dit bedrag vlak na de ontvangst daarvan door gebruikmaking van de bankpas van de betrokkene en het invoeren van de juiste pincode bij geldautomaten is opgenomen van zijn betaalrekening. Er is ook vastgesteld dat de limieten van de bankpas voor de opnames zijn verhoogd en dat het saldo van de betaalrekening voorafgaand aan de frauduleuze overboeking naar diens rekening € 0,- bedroeg.

De betrokkene heeft geen enkele plausibele verklaring gegeven over deze gang van zaken, terwijl dat gelet op de omvang van de verhoging van de opnamelimiet wel verwacht had mogen worden.



Voorbeeld uit de jurisprudentie (2)

In de sepotbrief van het Openbaar Ministerie staat dat de betrokkene wordt verdacht van 'overige horizontale fraude' en dat deze zaak wordt geseponneerd wegens onvoldoende bewijs.

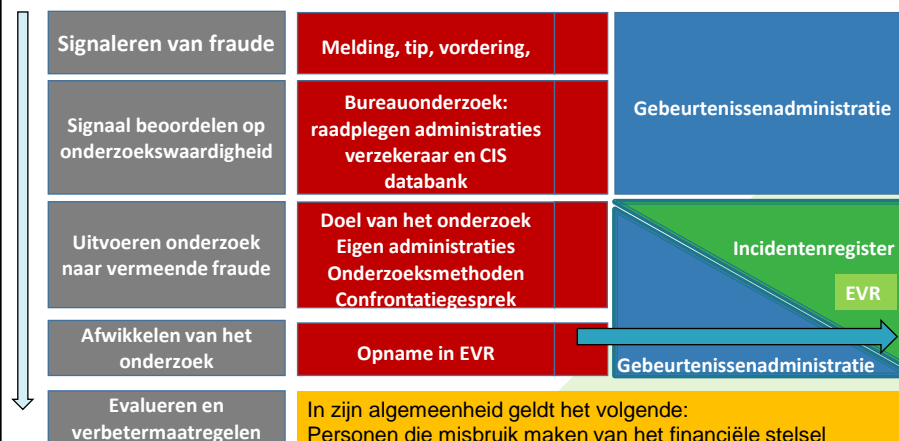
Herbeoordeling:

Het sepot ziet op andere strafbare gedragingen (namelijk: overige horizontale fraude) dan de strafbare gedraging die door de bank is geadministreerd (namelijk: schuldwitwassen). De feiten die door het OM zijn gewogen gaan uit van een andere verdenking.

Het sepot betekent dus niet dat geen sprake is van een zwaardere verdenking dan een redelijk vermoeden van schuld in de zin van het fungeren als geldezel. De registratie in EVR blijft staan.

(Uitspraak Geschillencommissie Financiële Dienstverlening nr. 2020-127).

3e criterium art. 5.2.1: Proportionaliteitstoets



Proportionaliteitstoets

- ▶ De financiële instelling moet bij de registratie in het EVR een proportionaliteitsafweging maken en bij de vraag voor welke duur, ook de belangen van de betrokkene meewegen.
- ▶ De aard van een incident rechtvaardigt in beginsel een opnameduur van 8 jaar in het EVR.
- ▶ Van deze opnameduur kan worden afgeweken in bijzondere omstandigheden, die door de financiële instelling worden beoordeeld.

Dubbele proportionaliteitstoets

- ▶ De betrokkene die verwijdering van een registratie wenst, zal moeten onderbouwen op grond waarvan hij te zwaar wordt geraakt in zijn belangen en waarom zijn belang zwaarder moet wegen dan het belang van financiële instelling bij voortduring of bij de duur van de registratie.
- ▶ Let op:
EVR-opname is GEEN straf. EVR dient ervoor om de toetser na een hit te attenderen dat de betrokkene mogelijk een risico vormt voor dienstverlening of indienstneming.

Delen in de lusten en de lasten

In deze zaak staat vast dat [A] mede namens zijn partner [B] bij een ingediende hypotheekaanvraag valselijk opgemaakte salarisspecificaties en werkgeversverklaringen heeft overgelegd.

Ook heeft [A] onder zijn partners naam online een kredietaanvraag bij de Rabobank ingediend, waarbij hij onjuiste inkomensgegevens van [B] heeft opgegeven.

Dit alles heeft hij zonder medeweten van [B] gedaan.

Is het terecht dat ook [B] wordt opgenomen in het EVR?

Delen in de lusten en de lasten

De rechter* laat de registratie van [B] in het EVR in stand. [B] heeft bij KvK een eenmanszaak ingeschreven, een autohandel. De onderneming is te bereiken is op het e-mailadres van [A] en draagt ook de naam van [A]. De rechter acht het niet aannemelijk dat deze eenmanszaak ook daadwerkelijk door [B] wordt gerund. [B] fungeert in feite als katvanger.

Verwijdering van [B's] persoonsgegevens uit EVR betekent de facto dat banken en verzekeringen financiële diensten aan de eenmanszaak zullen verlenen, zonder dat zij daarbij gealarmeerd worden door de registraties van [A] in het EVR

Gefingeerd dienstverband

BFM heeft 27 medewerkers in dienst en doet ondersteunende diensten doet voor 300 Verenigingen van Eigenaren

In deze zaak staat vast dat [A, de oprichter en DGA van BFM] aan een medewerker opdracht heeft gegeven om een gefingeerde werkgeversverklaring en arbeidsovereenkomst op te stellen op verzoek van de broer van [B] ten behoeve van [C].

[C, een kind van B] overlegde deze bescheiden in het kader van een hypotheekaanvraag bij SNS. De fraude komt uit en zowel [A] als [BFM] worden geregistreerd in EVR.

Is het terecht dat ook [BFM] wordt opgenomen in het EVR?



Wel met uw bedrijf maar niet met u

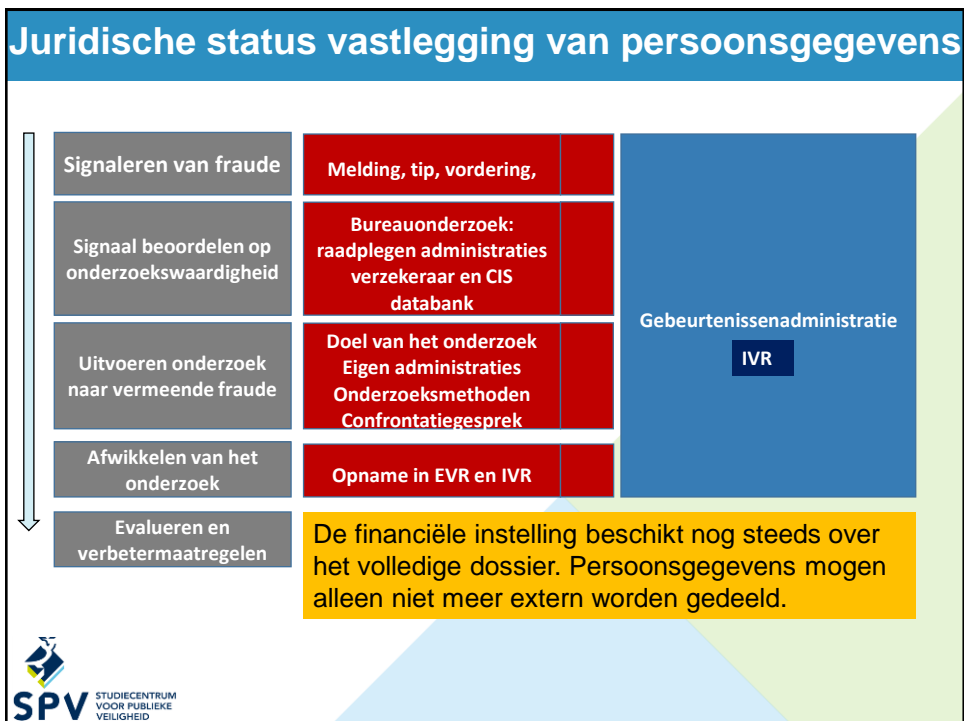
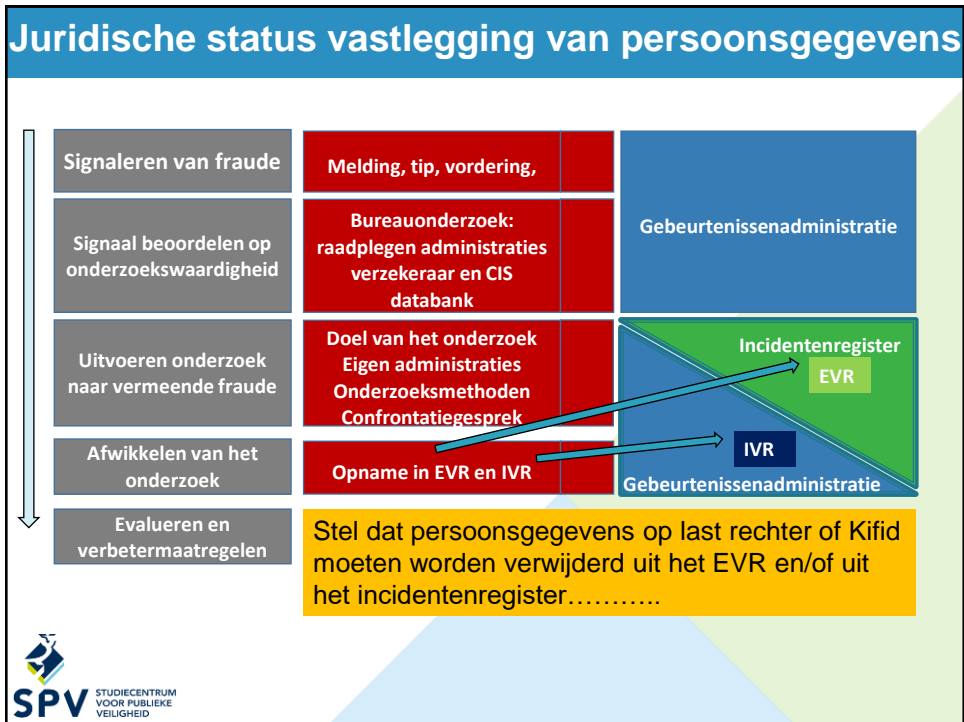
De rechter* onderkent dat de bedrijfsvoering door BFM ernstig wordt belemmerd en een groot gevaar loopt ten onder te gaan. Zij kan immers geen rekeningen meer openen voor de VvE's noch gemachtigde zijn op de bankrekeningen van de VvE's.

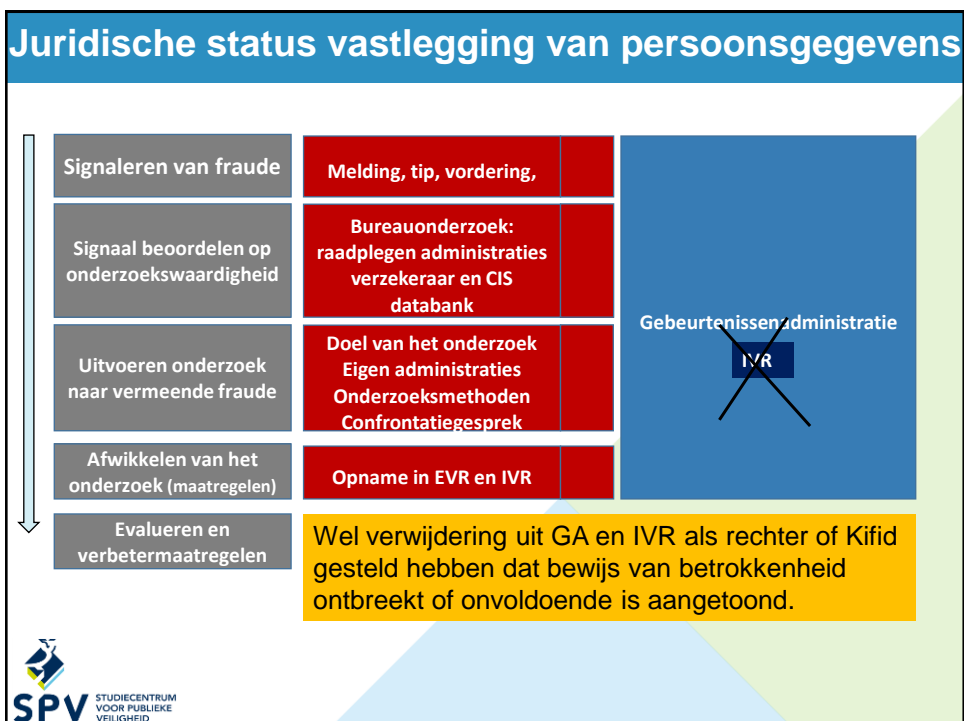
SNS heeft aangegeven de registratie van BFM te heroverwegen als [A] terugtreedt als DGA van BFM, wat de facto betekent dat hij zijn bedrijf moet verkopen.

De rechter kan zich vinden in het standpunt van SNS en laat de registratie van BFM in stand.

* Rechtbank Oost-Brabant 16 februari 2016,
ECLI:NL:RBOBR:2016:2529








Juridische status vastlegging van persoonsgegevens

Signaleren van fraude	Melding, tip, vordering,	X
Signaal beoordelen op onderzoekswaardigheid	Bureauonderzoek: raadplegen administraties verzekeraar en CIS databank	
Uitvoeren onderzoek naar vermeende fraude	Doel van het onderzoek Eigen administraties Onderzoeksmethoden Confrontatiegesprek	
Afwikkelen van het onderzoek (maatregelen)	Opname in EVR en IVR	
Evalueren en verbetermaatregelen	In dat geval hoeven de gegevens niet in zijn geheel te worden verwijderd, maar moet de zaak geheel geanonimiseerd worden: Geen op personen herleidbare gegeven meer in de onderzoeksadministratie!.	



SPV STUDECENTRUM VOOR PUBLIEKE VEILIGHEID



SPV STUDECENTRUM VOOR PUBLIEKE VEILIGHEID

Inzicht in Witwassen en Fraude

Toets

Vraag 1

Eén van de werkwijzen om geld wit te wassen en zogenaamd legale inkomsten te verkrijgen, is het sleutelen aan de inkomstenkant. 'Zwarte' criminele geldstromen worden op deze wijze als 'witte' legale geldstromen gepresenteerd.

Welke witwasmethode past hierbij?

- a) Een auto op naam van je schoonmoeder laten registreren.
- b) Een goed in het buitenland met contant crimineel geld kopen en vervolgens in Nederland verkopen.
- c) Als katvanger je bankrekening ter beschikking stellen aan een crimineel.

Vraag 2

Welke bewering is JUIST?

- a) Tegenover een goederenstroom staat altijd een geldstroom.
- b) Tegenover een goederenstroom staat meestal een geldstroom.
- c) Een onderzoek naar de geldstroom kan NIET bijdragen aan het afpakken van crimineel vermogen.

Vraag 3

Welke bewering is JUIST?

- a) FIU-Nederland onderzoekt ongebruikelijke transacties en initieert strafrechtelijke en fiscale onderzoeken.
- b) De politie heeft de directe beschikking over alle ongebruikelijke transacties die financiële instellingen melden.
- c) Een levensverzekeraar is NIET Wwft-plichtig.

Vraag 4

Is een makelaar in onroerend goed Wwft-plichtig?

- a) Ja, altijd.
- b) Nee, nooit.
- c) Ja, maar alleen als deze als zodanig is ingeschreven bij de KvK.

Vraag 5

Welke bewering over de Sanctiewet en -regelgeving is **JUIST**?

- a) Deze heeft ook betrekking op personen die van terroristische activiteiten worden verdacht.
- b) Alleen de Douane houdt toezicht op de naleving daarvan.
- c) Naast DNB en AFM houdt ook de belastingdienst toezicht op de naleving van het financiële gedeelte daarvan.

Vraag 6

Welke volgorde in het witwasproces is **JUIST**?

- a) Placement, Layering, Integration.
- b) Layering, Integration, Placement.
- c) Integration, Placement, Layering.

Vraag 7

Welke bewering over witwassen is **JUIST**?

- a) Voor witwassen is de dienstensector het meest geschikt.
- b) Voor witwassen is de bankensector ongeschikt.
- c) Witwassen komt in de industriële bedrijfssector regelmatig voor.

Vraag 8

Om een strafrechtelijk witwasartikel toe te kunnen passen, is een gronddelict nodig?

Wat moet de aard van dit gronddelict zijn?

- a) Een overtreding.
- b) Een overtreding en/ of een misdrijf.
- c) Een misdrijf.

Vraag 9

Wat geldt voor financiële instellingen voor het vastleggen van signalen van fraude?

- I. Als Veiligheidszaken een signaal van fraude ontvangt, wordt dit in eerste instantie vastgesteld in de gebeurtenissenadministratie.
 - II. Het signaal wordt door Veiligheidszaken direct vastgelegd in het incidentenregister.
- a) alleen stelling I is juist.
 - b) alleen stelling II is juist.
 - c) stellingen I en II zijn onjuist.

Vraag 10

Wat is juist ten aanzien van het plaatsen van iemand in het extern verwijzingsregister (EVR)?

- a) Voor afgaand aan plaatsing in EVR moet hoor- en wederhoor worden toegepast.
- b) Na plaatsing in EVR moet altijd aangifte worden gedaan bij de politie.
- c) Voor plaatsing in EVR moet in voldoende mate vast staan dat iemand betrokken is bij de onacceptabele gedraging.

Vraag 11

Wat is juist ten aanzien van de Algemene Verordening Gegevensbescherming (AVG)?

- a) In aanvulling op de Wet bescherming persoonsgegevens (Wbp) bepaalt de AVG dat een financiële instelling een functionaris voor gegevensbescherming (FG) bij de afdeling Veiligheidszaken moet aanwijzen.
- b) Aan die fraudeur wiens persoonsgegevens zijn vastgelegd in het incidentenregister moet informatie worden dat vastlegging van diens persoonsgegevens in het incidentenregister heeft plaatsgevonden.
- c) Onder de AVG moet de gebeurtenissenadministratie gemeld bij de Autoriteit Persoonsgegevens.

Vraag 12

Wat is juist ten aanzien van het plaatsen van iemand in het intern verwijzingsregister (IVR) van een financiële instelling?

- a) Voorafgaand aan het gebruik van een IVR moet de Autoriteit Persoonsgegevens een vergunning afgeven.
- b) Wanneer sprake is van de verwerking van strafrechtelijke persoonsgegevens moet bij plaatsing in IVR aangifte worden gedaan bij een politieambtenaar.
- c) Een financiële instelling bepaalt zelf welke criteria het hanteert als zij iemand in het IVR wil opnemen. Dat geldt ook voor de bewaarduur van persoonsgegevens in het IVR.

Vraag 13

Wat is juist ten aanzien van de Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG)?

- a) In aanvulling op de Wet op het financieel toezicht (Wft) bepaalt de UAVG dat een financiële instelling een afdeling Veiligheidszaken moet hebben.
- b) De UAVG biedt de mogelijkheid voor de Autoriteit Persoonsgegevens om vergunningen af te geven voor het verwerken van zogenaamde "Strafrechtelijke persoonsgegevens" voor derden.
- c) Om als financiële instelling mee te kunnen doen met EVR moet de financiële instelling een voorafgaande raadpleging doen bij de Autoriteit Persoonsgegevens.

Vraag 14

Wat geldt voor de aansprakelijkheid van de bank als een niet-rekeninghouder schade lijdt als gevolg van CEO-fraude?

- I. De bank kan aansprakelijk worden gehouden als medewerkers van de bank niet adequaat handelen na een alert. De bank kan dan verweten worden dat zij niet heeft gehandeld zoals in het maatschappelijk verkeer betaamt.
 - II. De bank is aansprakelijk omdat de criminelen door de fraude inbreuk hebben gemaakt op eigendomsrechten van een rekeninghouder.
- a) alleen stelling I is juist.
 - b) alleen stelling II is juist.
 - c) stellingen I en II zijn onjuist.

Vraag 15

Fraude komt als zodanig niet voor in het Wetboek van strafrecht. Het is meer een verzamelnaam die omschreven wordt met een aantal aspecten die benadrukken dat sprake is van fraude.

Welke van de volgende aspecten horen bij de omschrijving van fraude?

Er kunnen meerdere juiste antwoorden mogelijk zijn.

- a) onrechtmatig voordeel.
- b) onjuiste voorstelling van zaken.
- c) opzettelijk.

Vraag 16

Een bank kan aansprakelijk worden gehouden voor schade als een rekeninghouder fraudeert en derden dupeert. Van de bank wordt verwacht dat het adequaat reageert op een patroon van afwijkende en ongebruikelijke betalingen. Nadat de bank subjectieve wetenschap heeft verkregen moeten medewerkers van de bank bepaald gedrag vertonen.

Wat kan zoal verwacht worden van medewerkers?

Er kunnen meerdere juiste antwoorden mogelijk zijn.

- a) Iemand informeren of waarschuwen.
- b) Zich niet laten afschepen door de klant.
- c) De klant om opheldering vragen.

Inzicht in Witwassen en Fraude

Antwoorden per vraag

Vraag 1

Eén van de werkwijzen om geld wit te wassen en zogenaamd legale inkomsten te verkrijgen, is het sleutelen aan de inkomstenkant. 'Zwarte' criminele geldstromen worden op deze wijze als 'witte' legale geldstromen gepresenteerd.

Welke witwasmethode past hierbij?

- a) Een auto op naam van je schoonmoeder laten registreren.
- b) Een goed in het buitenland met contant crimineel geld kopen en vervolgens in Nederland verkopen.
- c) Als katvanger je bankrekening ter beschikking stellen aan een crimineel.

→
Juiste antwoord

Vraag 2

Welke bewering is JUIST?

- Juiste antwoord
- a) Tegenover een goederenstroom staat altijd een geldstroom.
 - b) Tegenover een goederenstroom staat meestal een geldstroom.
 - c) Een onderzoek naar de geldstroom kan NIET bijdragen aan het afpakken van crimineel vermogen.

Vraag 3

Welke bewering is JUIST?

- Juiste antwoord
- a) FIU-Nederland onderzoekt ongebruikelijke transacties en initieert strafrechtelijke en fiscale onderzoeken.
 - b) De politie heeft de directe beschikking over alle ongebruikelijke transacties die financiële instellingen melden.
 - c) Een levensverzekeraar is NIET Wwft-plichtig.

Vraag 4

Is een makelaar in onroerend goed Wwft-plichtig?

→
Juiste antwoord

- a) **Ja, altijd.**
- b) Nee, nooit.
- c) Ja, maar alleen als deze als zodanig is ingeschreven bij de KvK.

Vraag 5

Welke bewering over de Sanctiewet en -regelgeving is **JUIST**?

→
Juiste antwoord

- a) **Deze heeft ook betrekking op personen die van terroristische activiteiten worden verdacht.**
- b) Alleen de Douane houdt toezicht op de naleving daarvan.
- c) Naast DNB en AFM houdt ook de belastingdienst toezicht op de naleving van het financiële gedeelte daarvan.

Vraag 6

Welke volgorde in het witwasproces is JUIST?

- Juiste antwoord a) Placement, Layering, Integration.
b) Layering, Integration, Placement.
c) Integration, Placement, Layering.

Vraag 7

Welke bewering over witwassen is JUIST?

- Juiste antwoord a) Voor witwassen is de dienstensector het meest geschikt.
b) Voor witwassen is de bankensector ongeschikt.
c) Witwassen komt in de industriële bedrijfssector regelmatig voor.

Vraag 8

Om een strafrechtelijk witwasartikel toe te kunnen passen, is een gronddelict nodig?

Wat moet de aard van dit gronddelict zijn?

- a) Een overtreding.
- b) Een overtreding en/ of een misdrijf.
- c) Een misdrijf.

Vraag 9

Wat geldt voor financiële instellingen voor het vastleggen van signalen van fraude?

- I. Als Veiligheidszaken een signaal van fraude ontvangt, wordt dit in eerste instantie vastgesteld in de gebeurtenissenadministratie.
- II. Het signaal wordt door Veiligheidszaken direct vastgelegd in het incidentenregister.

- a) alleen stelling I is juist.
- b) alleen stelling II is juist.
- c) stellingen I en II zijn onjuist.

Vraag 10

Wat is juist ten aanzien van het plaatsen van iemand in het extern verwijzingsregister (EVR)?

- a) Voorafgaand aan plaatsing in EVR moet hoor- en wederhoor worden toegepast.
- b) Na plaatsing in EVR moet altijd aangifte worden gedaan bij de politie.
- c) Voor plaatsing in EVR moet in voldoende mate vast staan dat iemand betrokken is bij de onacceptabele gedraging.

Juiste antwoord

Vraag 11

Wat is juist ten aanzien van de Algemene Verordening Gegevensbescherming (AVG)?

- a) In aanvulling op de Wet bescherming persoonsgegevens (Wbp) bepaalt de AVG dat een financiële instelling een functionaris voor gegevensbescherming (FG) bij de afdeling Veiligheidszaken moet aanwijzen.
- b) Aan die fraudeur wiens persoonsgegevens zijn vastgelegd in het incidentenregister moet informatie worden dat vastlegging van diens persoonsgegevens in het incidentenregister heeft plaatsgevonden.
- c) Onder de AVG moet de gebeurtenissenadministratie gemeld bij de Autoriteit Persoonsgegevens.

Juiste antwoord

Vraag 12

Wat is juist ten aanzien van het plaatsen van iemand in het intern verwijzingsregister (IVR) van een financiële instelling?

- a) Voorafgaand aan het gebruik van een IVR moet de Autoriteit Persoonsgegevens een vergunning afgeven.
- b) Wanneer sprake is van de verwerking van strafrechtelijke persoonsgegevens moet bij plaatsing in IVR aangifte worden gedaan bij een politieambtenaar.
- c) Een financiële instelling bepaalt zelf welke criteria het hanteert als zij iemand in het IVR wil opnemen. Dat geldt ook voor de bewaarduur van persoonsgegevens in het IVR.

→
Juiste antwoord

Vraag 13

Wat is juist ten aanzien van de Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG)?

- a) In aanvulling op de Wet op het financieel toezicht (Wft) bepaalt de UAVG dat een financiële instelling een afdeling Veiligheidszaken moet hebben.
- b) De UAVG biedt de mogelijkheid voor de Autoriteit Persoonsgegevens om vergunningen af te geven voor het verwerken van zogenaamde "Strafrechtelijke persoonsgegevens" voor derden.
- c) Om als financiële instelling mee te kunnen doen met EVR moet de financiële instelling een voorafgaande raadpleging doen bij de Autoriteit Persoonsgegevens.

→
Juiste antwoord

Vraag 14

Wat geldt voor de aansprakelijkheid van de bank als een niet-rekeninghouder schade lijdt als gevolg van CEO-fraude?

- I. De bank kan aansprakelijk worden gehouden als medewerkers van de bank niet adequaat handelen na een alert. De bank kan dan verweten worden dat zij niet heeft gehandeld zoals in het maatschappelijk verkeer betaamt.
- II. De bank is aansprakelijk omdat de criminelen door de fraude inbreuk hebben gemaakt op eigendomsrechten van een rekeninghouder.

- Juiste antwoord
- a) alleen stelling I is juist.
 - b) alleen stelling II is juist.
 - c) stellingen I en II zijn onjuist.

Vraag 15

Fraude komt als zodanig niet voor in het Wetboek van strafrecht. Het is meer een verzamelnaam die omschreven wordt met een aantal aspecten die benadrukken dat sprake is van fraude.

Welke van de volgende aspecten horen bij de omschrijving van fraude?

Er kunnen meerdere juiste antwoorden mogelijk zijn.

- Juiste antwoord
- Juiste antwoord
- Juiste antwoord
- a) onrechtmatig voordeel.
 - b) onjuiste voorstelling van zaken.
 - c) opzettelijk.

Vraag 16

Een bank kan aansprakelijk worden gehouden voor schade als een rekeninghouder fraudeert en derden dupeert. Van de bank wordt verwacht dat het adequaat reageert op een patroon van afwijkende en ongebruikelijke betalingen. Nadat de bank subjectieve wetenschap heeft verkregen moeten medewerkers van de bank bepaald gedrag vertonen.

Wat kan zoal verwacht worden van medewerkers?

Er kunnen meerdere juiste antwoorden mogelijk zijn.

- Juiste antwoord a) Iemand informeren of waarschuwen.
- Juiste antwoord b) Zich niet laten afschepen door de klant.
- Juiste antwoord c) De klant om opheldering vragen.



SECURITY & RECHT

Eigendomsrechten

Felix Olijslager

Copyright 2022 maart)

Alle rechten voorbehouden. Dit document bevat de slides die door de docenten van SPV worden gebruikt tijdens de lessen Straff(proces)recht voor financiële instellingen (SPR) om de kracht van hun boodschap bij te zetten. De slides worden ofwel voorafgaand ofwel na afloop van de betreffende les aan de deelnemers van de opleiding SPR beschikbaar gesteld. Niets uit dit document mag worden openbaar gemaakt en/of gebruikt worden door anderen dan de auteur mr. F.B.M. Olijslager, in enige vorm of op enige wijze, hetzij elektronisch, mechanisch, door fotokopieën, opnamen of enige andere wijze, zonder voorafgaande schriftelijke toestemming van hem. Ook mogen de slides niet gebruikt worden voor opleidingen, trainingen en cursussen als mr. F.B.M. Olijslager niet zelf bij de opleiding, cursus of training betrokken is.