



NOREA & ISACA Young Prof Event

# Anti Money Laundering in a digital world

11 maart 2020

Ellen Klijstra

Hoe wordt financiële criminaliteit bestreden? Welke technieken worden daarvoor gebruikt en wat is daarin de rol van de banken? En hoe zit het met de samenwerking tussen de banken, de Financial Intelligence Unit-Nederland (FIU), de Fiscale Inlichtingen en OpsporingsDienst (FIOD) en het OM? Een greep uit de vragen die bijna dagelijks via het nieuws passeren: dinsdag 18 februari 2020 vond het NOREA & ISACA YP event 'Anti Money Laundering in a digital world' plaats in de ABN Amro Circl in Amsterdam. Met 52 deelnemers was het een volle zaal en een aandachtig oor voor dit onderwerp. Medewerkers van FIOD en van de afdeling Detecting Financial Crime van ABN Amro spraken over het opsporen van witwassen dankzij technieken zoals data-analyse, machine learning en algoritmes.

*Anti money laundering* is een *hot topic* en de instanties die de taak hebben witwassen tegen te gaan, te signaleren en op te sporen, vervullen een maatschappelijke functie. Een net van actoren en samenwerking: de poortwachtersfunctie van banken, financieel rechercheurs, instellingen zoals de FIOD en de FIU, het toezicht vanuit DNB, maar ook betrokkenheid van het OM. De *crime fighters* zijn niet aan te slepen.

## Financiële criminaliteit opsporen met data-analyse

Hoe kan je in dit web financiële criminaliteit opsporen? En welke IT-middelen gebruik je daarvoor? De spreker van de FIOD liet in zijn presentatie zien hoe je met data-analyse debit- en credittransacties duidelijk in kaart kan brengen, als stap om mogelijke financiële criminaliteit op te sporen. Gegevens zoals het aantal transacties met dezelfde kaart, de plekken en tijdstippen waar deze transacties plaatsvinden en het bedrag worden geanalyseerd. Door deze gegevens in kaart te brengen en te visualiseren breng je zichtbare patronen aan het licht. Dit leidt naar een interessante trail. Maar wat is normaal 'gedrag' van een debit- of creditcard? En hoe verhoudt deze trail zich tot het gedefinieerde normale gedrag? Een enorme bak met data van meer dan 136 miljoen transacties wordt op zo'n manier met data-analyse afgepeld, leidend tot interessante, afwijkende en mogelijk verdachte activiteiten.

Wat normaal gebruik is van een debit- en creditcard, is al lastig genoeg te bepalen door de vele verschillende leefstijlen. Extra ingewikkeld wordt het als je financiële constructies in kaart wilt brengen. De authenticiteit van je evidence nagaan – een basaal element dat we als IT-auditor allemaal kennen – blijkt ook hier weer essentieel te zijn. Denk bijvoorbeeld aan het beoordelen van facturen en hoe de boekingen hiervan in de systemen zijn verwerkt. Het wordt al snel duidelijk dat data key is voor het opsporen van financiële criminaliteit. Het begint heel simpel met de vraag: ‘wat zien we hier nu?’

## Algoritmes – blijven de *good guys* achter lopen?

Data-analyse is een methode waarmee IT-auditors al langer bekend zijn, maar wanneer we een stapje verder gaan komen machine learning en algoritmes tegen. De sprekers van Detecting Financial Crime van ABN geven een inkijkje hoe een bank witwassen opspoot door onder andere transacties te monitoren. Noem het *Transaction Monitoring 2.0*, want dit model past algoritmes toe en leert van data. Een kijkje in de wisselwerking tussen criminelen en banken: criminelen willen geld witwassen, of terrorisme financieren. Om niet op te vallen met deze geldstromen bedenken ze onopvallende manieren om dit te kunnen doen. De bank reageert hierop en past nieuwe methodes toe om de ‘onopvallende manier’ te achterhalen en in het vervolg tijdig te kunnen detecteren. In reactie hierop stappen de witwassers over op een nieuwe manier om alsnog onopvallend te blijven. Deze cirkel blijft zich herhalen en het zijn vooral de witwassers die voorop lopen. Zij zijn het immers, die nieuwe methodes blijven bedenken en toepassen. Hierdoor lopen de *good guys* in de praktijk altijd achter. De kunst is nu om deze achterstand zo klein mogelijk te houden. Dit vereist dat de gebruikte opsporingstechnieken snel en gemakkelijk de veranderende omgeving moeten kunnen bijbenen. Het is daardoor niet meer dan logisch om de oplossing te zoeken in *machine learning*.

## Model is één, praktijk is twee

Maar dan komen we onvermijdelijk een aantal uitdagingen tegen, want hoe gaan we om met zaken als (etnisch) profileren, het gebruik van privégegevens of discriminatie? Een model moet niet alleen witwassen kunnen opsporen, en daarmee voldoen aan de Wet ter voorkoming van witwassen en financieren van terrorisme (Wwft), maar moet ook voldoen aan de AVG. Dit is nog een heikel punt omdat we momenteel in de situatie zitten dat het *design* van zo’n model óf *compliant* is met de Wwft, óf met de AVG. Wordt dat kiezen tussen twee vuren? Nee, legt een van de sprekers uit, we zijn nu bezig om gesprekken te voeren met andere banken, DNB en Autoriteit Persoonsgegevens om dit knelpunt op te lossen.

Wat is onze rol als IT-auditor in het auditen van zo'n model? Hoe weten we zeker dat we alle risico's goed in kaart hebben gebracht? Zoals het etnisch profileren, of dat het model AVG compliant is? Deze vragen zitten niet direct in een beoordeling van *general IT controls of application controls* besloten, maar zijn wel cruciaal. Deze sessie gaf dus weer eens aan hoe noodzakelijk het is dat wij IT-auditors blijven met de ontwikkeling van IT. Alleen op de hoogte zijn is niet voldoende: eigenlijk moeten we er al boven staan.

## Veiligheid van Nederland: samen sterk

Het wordt tijdens deze middag ook duidelijk hoe dicht IT bij de maatschappij staat en een maatschappelijke rol vervult. Soms kan het abstract lijken als we interfaces aan het toetsen zijn, maar deze voorbeelden geven goed weer wat voor maatschappelijke impact en gevolgen ermee verbonden zijn. Een kernwaarde die zowel de FIOD als ABN Amro benoemen is 'Nederland een stukje veiliger maken'. Het is mooi en uniek om te zien dat sterk verschillende organisaties – toezichthouders en opsporingsinstanties in het publieke domein, respectievelijk private partijen in het bankwezen – elkaar opzoeken om samen hetzelfde doel na te streven. Een gebied in ontwikkeling waar we nog veel over gaan horen!

Dit event werd georganiseerd door de Young Prof- commissie van NOREA en ISACA. Het doel van deze commissie is om Young Prof (aankomend) RE's bij elkaar te brengen en kennis te delen, met elkaar en met externe experts. De commissie organiseert geregeld events over uiteenlopende onderwerpen. Het onderwerp verschilt per event, maar is altijd relevant voor IT-auditors. Alle YP's zijn dan ook van harte welkom om deze bij te wonen!



### E.W.H. (Ellen) Klijnstra MSc LLM | IT-auditor bij AMRO / Group Audit

Ellen Klijnstra begon als IT-auditor bij KPMG en is sinds begin 2019 werkzaam bij ABN AMRO, Group Audit. Ze houdt zich bezig met audits gerelateerd aan *anti money laundering*, *customer due diligence* en *know your customer*. Haar RE-opleiding aan de Erasmus Universiteit Rotterdam heeft ze in maart 2020 afgerond. Ze is actief als commissielid in de NOREA / ISACA Young Prof-commissie.