De toepassing van technologie in het klantacceptatie- en transactie-monitoringsproces ter bestrijding van financieel-economische criminaliteit

Dr. J.S. van der Graaf

1. Inleiding

Technologie is in de wereld om ons heen niet meer weg te denken. Zo ook in de financiële sector waar instellingen de afgelopen decennia in verregaande mate zijn gaan bouwen op technologie om gevoelige data en kritieke infrastructuren te beheren. Technologische toepassingen spelen ook een steeds grotere rol waar het gaat om financieel-economische criminaliteit (FEC).[1] Zowel in processen om te voorkomen dat financiële instellingen betrokken raken bij FEC als juist ook in nieuwe of steeds complexere vormen van aan FEC verbonden risico's, bijvoorbeeld cybercriminaliteit of witwassen met behulp van virtuele valuta.

Steeds vaker spelen financiële instellingen, onder de noemer van regulatory technology (hierna: RegTech), en RegTech-dienstverleners in op de wens om voortgang te boeken wat betreft mogelijkheden, snelheid en efficiëntie in het detecteren van FEC en om hierover te rapporteren. Daarnaast vormt de behoefte om nalevingskosten beter beheersbaar te maken een belangrijke reden voor de huidige aandacht voor RegTech.

1 In dit artikel wordt de term financieel-economische criminaliteit gebruikt om te refereren aan vormen van criminaliteit die raken aan het financiële systeem doordat zij deze misbruiken voor oneigenlijke doelen en het plegen van een strafbaar feit. Te denken valt aan witwassen, corruptie (omkoping), financiering van terrorisme, handel met voorwetenschap, niet-naleven van sancties, verduistering, oplichting en valsheid in geschrifte (zie ook het factsheet van De Nederlandsche Bank 'De aanpak van financieel-economische criminaliteit').

Naast de invloed van technologische toepassingen op de manier waarop financiële instellingen voldoen aan wet- en regelgeving, hebben technologische toepassingen ook hun weerslag op de manier waarop toezicht wordt gehouden op deze instellingen.[2] In dit artikel wordt ingegaan op de mogelijkheden van het gebruiken van technologische toepassingen in het klantacceptatie- en transactiemonitoringsproces voor het mitigeren van risico's ten aanzien van FEC. Daarnaast zullen de uitdagingen die hiermee gepaard gaan voor financiële instellingen, waaronder voor de rol van de compliance officer, en toezichthouders worden belicht.

2. De potentie van RegTech

De term RegTech wordt veelal gebruikt om te duiden op technologische toepassingen voor het bewerkstelligen van compliance. RegTech is geenszins een nieuwe ontwikkeling, maar wel een die in de financiële sector een impuls heeft gekregen na de financiële crisis van 2007-2008 resulterend in toegenomen uitgaven aan compliance, waaronder aan de bestrijding van FEC.[3] Dit nodigt instellingen uit om initiatieven te ontplooien en implementeren om op efficiëntere en meer kostenbesparende wijze te voldoen aan regels.

Instellingen kunnen RegTech op verschillende terreinen toepassen. Zo zijn er RegTech-oplossingen die gericht zijn op het op zichzelf en geautomatiseerd identificeren van veranderingen in het regelgevend landschap of die gericht zijn op het voldoen aan rapportagevereisten uit prudentiële wet- en regelgeving, bijvoorbeeld ten behoeve van kapitaal- en liquiditeitseisen. In dit artikel ligt de nadruk echter op technologische toepassingen in de bestrijding van FEC.

3. FEC en RegTech

Financiële instellingen hebben een wettelijk verankerde poortwachtersfunctie om te voorkomen dat zij betrokken raken bij FEC zoals witwassen en financiering van terrorisme. Onder andere de Wet op het financieel toezicht (Wft), de Pensioenwet, de Wet toezicht trustkantoren (Wtt), de Wet ter voorkoming van witwassen en financieren van terrorisme (Wwft) en de Sanctiewet 1977 (Sw) bevatten verplichtingen voor financiële instellingen ten aanzien van het identificeren van risico's die zij lopen op het begaan of faciliteren van FEC en het nemen van maatregelen om deze risico's te mitigeren.

2 Naast RegTech is hier ook FinTech van belang, een term die refereert aan de toepassing van technologie ten behoeve van innovaties in het aanbieden van financiële producten en diensten.

3 Zie bijvoorbeeld PWC 'Global Economic Crime Survey 2016 – Financial Services Industry Insights'.

De beheersing van risico's verbonden aan FEC vereist betrokkenheid van compliance professionals met specifieke vakkennis, met name daar waar verdergaand onderzoek noodzakelijk is. De kosten om deze gespecialiseerde kennis in te zetten zijn voor instellingen hoog, terwijl tegelijkertijd menselijke fouten en inefficiëntie het proces van risicobeheersing blijven beïnvloeden. In dit deel zal worden ingegaan op RegTech-initiatieven gericht op het beperken van kosten en kwetsbaarheden in twee kernprocessen die cruciaal zijn in de bestrijding van FEC namelijk het klantacceptatie- en transactiemonitoringsproces.

3.1 De toekomst van onboarding

Het kennen van de klant is een cruciaal onderdeel van financiële dienstverlening. Waar dit voor instellingen lange tijd relatief eenvoudig was met veel persoonlijk contact, is dit onder invloed van economische, maatschappelijke én technologische ontwikkelingen in enkele decennia sterk veranderd. Bovendien verwachten consumenten steeds meer op afstand te kunnen doen. Naast het belang van het kennen van de klant voor de integere bedrijfsvoering van instellingen, is het specifieke belang voor het bestrijden van witwassen en terrorismefinanciering, het voldoen aan sanctieregels en het voorkomen van fiscale fraude, steeds meer op de voorgrond gekomen en geformaliseerd als vereiste in financiële wet- en regelgeving.[4]

Een belangrijke rol in het kennen van de klant speelt het klantacceptatieproces waarmee het onderzoek naar de klant wordt verricht voordat een instelling een zakelijke relatie aangaat of een transactie uitvoert. In dit onderzoek is het noodzakelijk om informatie uit verschillende bronnen te raadplegen en te analyseren om onder andere de identiteit van een zakelijke relatie en uiteindelijk belanghebbende vast te stellen en de identiteit van een relatie te verifiëren. Met name in complexe gevallen, bijvoorbeeld bij potentiële klanten die actief zijn in meerdere jurisdicties, vormt klantacceptatie een intensief proces. Het opvragen van documenten, gegevens of informatie, het controleren van de juistheid hiervan en het vastleggen van verkregen gegevens, kost veel tijd. Dit is dan ook de reden dat instellingen inventariseren en experimenteren met technologische vernieuwingen in het klantacceptatieproces.

Instellingen, al dan niet individueel of gezamenlijk, zijn in toenemende mate op zoek naar efficiëntere manieren van datavergaring en verificatie van deze data door deze naast data uit andere bronnen te leggen. Externe partijen die data uit verschillende bronnen aggre-

4 Een belangrijk startpunt van deze formalisering vormt reeds het Basel Statement of Principles uit 1988. Hierin werd gesteld dat het vertrouwen in de financiële sector ondermijnd wordt door financieel-economische criminaliteit. Het identificeren van klanten wordt genoemd als één van de manieren om dit tegen te gaan. In vervolg hierop noemde ook de Recommendations van de Financial Action Task Force uit april 1990 het belang van het identificeren van klanten en hun uiteindelijk belanghebbenden.

geren en deze op een centrale plek aanbieden voor het uitvoeren van klantonderzoeken worden daarbij steeds vaker gezien als de weg vooruit.[5]

Op de langere termijn kan distributed ledger-technologie[6], met blockchain als belangrijkste verschijningsvorm, een belangrijke rol gaan spelen in het samenbrengen van zogenaamde 'know-your-customer'-data.[7] Met behulp van distributed ledger-technologie kan data in een gezamenlijk netwerk worden bijgehouden door verschillende partijen, waaronder zelfs mogelijkerwijs publieke instanties als belastingautoriteiten en toezichthouders. Belangrijke vragen bij het gebruiken van een uniforme infrastructuur met decentrale opslag van data zijn wel hoe data wordt gevalideerd en wie de toegang tot bepaalde data bepaalt, bijvoorbeeld in geval van het klantacceptatieproces.

Andere technieken die in het klantacceptatieproces worden onderzocht hebben betrekking op biometrische technieken. Deze technieken kunnen in het bijzonder een rol gaan spelen bij identificatie en verificatie doordat dit gemakkelijker op afstand kan plaatsvinden met methoden die in andere domeinen, zoals binnenlandse veiligheid, reeds worden toegepast in de vorm van gezichts-, stem-, vingerafdruk- en irisherkenning. Huidige klantacceptatieprocessen leunen sterk op documentatie voor identificatie en verificatie, maar met de toepassing van biometrie zou het klantacceptatieproces kunnen opschuiven naar identificatie en verificatie (mede) op basis van unieke biologische kenmerken die meer betrouwbaar en minder fraudegevoelig zijn.

Naar aanleiding van identificatie en verificatie met biometrie, zou ook het gebruik van digitale identiteit een rol kunnen gaan spelen waarbij het proces van identificatie en verificatie slechts eenmalig hoeft plaats te vinden en vervolgens een digitale identiteit ontstaat die gebruikt kan worden bij iedere transactie in het financiële stelsel. De eerste eenmalige identificatie en verificatie weegt daarbij desalniettemin nog zwaarder en de vraag is ook welke partij hiervoor dan verantwoordelijk is en de kosten zal dragen.[8]

5 Voorbeelden hiervan zijn het KYC Registry van SWIFT gelanceerd in 2014 of initiatieven vanuit een partij als kyc.com.

6 Zie algemeen over de mogelijkheden van de distributed ledger-technologie bijvoorbeeld het DNBulletin 'Blockchaintechnologie biedt kansen' (31 augustus 2017).

7 KYC Chain (kyc-chain.com) is een dergelijk nieuw platform dat gebruik maakt van distributed ledger-technologie.

8 In het kader van de nieuwe betaalrichtlijn Payment Services Directive (PSD2), zijn vragen over het delen van klantgegevens ook reeds urgent voor instellingen. Na toestemming van klanten worden banken met de implementatie van PSD2 verplicht gegevens die zij hebben vergaard te delen met andere dienstverleners.

3.2 Transactiemonitoring en kunstmatige intelligentie

Het monitoren van de activiteiten en transacties van klanten en het melden van ongebruikelijke transacties bij de Financial Intelligence Unit (FIU), vormt een cruciaal proces in het voorkomen van FEC zodra een klantrelatie tot stand is gekomen. Monitoring kan op verschillende wijzen worden ingericht bijvoorbeeld in de vorm van gerichte controles op bepaalde rekeningen of bij bepaalde transacties of in de vorm van handmatige monitoring. Een belangrijke plek binnen financiële instellingen wordt echter ingenomen door transactiemonitoringssystemen die in het geval bepaalde, ongebruikelijke transacties of patronen in transacties plaatsvinden automatisch een alert genereren.

Detectieregels, of business rules, met daarin scenario's en grenswaarden, filteren in een transactiemonitoringssysteem ongebruikelijke transacties uit de miljoenen transacties die dagelijks plaatsvinden bij de grotere instellingen. Instellingen worden daarbij nog veelvuldig geconfronteerd met 'false positives' en blijven kwetsbaar voor 'false negatives'. Om het proces van transactiemonitoring efficiënter te maken, hebben instellingen de afgelopen jaren steeds meer werk gemaakt van intelligente transactiemonitoring waarbij een transactieprofiel van een klant wordt opgesteld waartegen iedere nieuwe transactie wordt getoetst. Transacties die buiten het verwachte patroon vallen worden nader onderzocht om na te gaan of deze als ongebruikelijk dienen te worden aangemerkt en gemeld te worden aan de FIU.

In een intelligent transactiemonitoringssysteem wordt door instellingen ook geëxperimenteerd met kunstmatige intelligentie met als doel de aanscherping van detectieregels. Op allerlei terreinen wordt kunstmatige intelligentie toegepast waarbij innovatieve, (zelf) lerende computers in staat zijn te reageren op allerlei data en gedragingen. Op basis daarvan kunnen deze computers taken zelfstandig uitvoeren en beslissingen nemen. Toegepast in de wereld van transactiemonitoring kan met behulp van kunstmatige intelligentie een detectiesysteem worden ingericht dat zelf kan leren bepaalde afwijkende alsook nieuwe, ongebruikelijke patronen te ontdekken. Daarmee kan met kunstmatige intelligentie in een veel grotere dataset worden gezocht naar verbanden die niet direct of helemaal niet duidelijk zichtbaar zouden worden wanneer enkel onderzoek plaatsvindt vanuit een menselijk oog.

Transactiemonitoring met behulp van kunstmatige intelligentie is voor nu toekomstmuziek. Bovendien zal het ook niet direct voor alle instellingen een relevante ontwikkeling zijn. Afhankelijk van de dienstverlening, de omvang van het aantal transacties en het type cliënten, zal de rol van geavanceerde transactiemonitoringtechnieken meer of minder relevant zijn. Bijvoorbeeld voor een instelling met een eenvoudig bedrijfsmodel zal de investering in kunstmatige intelligentie allicht een stap te ver zijn. Voor dergelijke instellingen zal het samenwerken met andere instellingen op het terrein van transactie-

monitoring wel een uitkomst kunnen bieden, wellicht wederom met behulp van distributed ledger-technologie.

4. Risico's rond de toepassing van RegTech in de bestrijding van FEC

Onbedoelde neveneffecten zijn waar het gaat om risico's en de beheersing ervan een veelbesproken onderwerp. Voor wat betreft de mogelijkheden van RegTech om verbeteringen te bewerkstellingen in de beheersing van risico's op FEC, geldt eveneens dat technologische toepassingen in zichzelf ook weer risico's met zich meebrengen. Eén van deze risico's betreft het risico dat het toenemende gebruik van technologie, instellingen juist ook weer kwetsbaar maakt voor misbruik. Het gebruik van RegTech-toepassingen kan FEC uitlokken, bijvoorbeeld waar oplossingen gericht zijn op het bij elkaar brengen en opslaan van grote hoeveelheden klantdata zoals hierboven besproken. Deze, veelal privacygevoelige, bij elkaar gebrachte data zal eveneens een aantrekkelijke bron zijn voor misbruik voor criminele doeleinden.

Een ander risico van RegTech is gelegen in de mate waarin instellingen zich tot op zekere hoogte afhankelijk maken van derde partijen voor de beheersing van risico's op FEC. Waar instellingen er regelmatig voor kiezen zelf onderzoek te doen naar RegTech-oplossingen en het bouwen van applicaties en toepassingen, is het voor instellingen ook aantrekkelijk om een beroep te doen op een externe partij met reeds aanwezige gespecialiseerde technologische kennis en middelen. RegTech-ontwikkelingen hebben inmiddels geleid tot een hele industrie van dienstverleners gespecialiseerd op dit terrein. Daarbij krijgen deze dienstverleners toegang tot gevoelige data zowel van instellingen als van hun klanten. Hoe hierbij wordt omgegaan met privacy is een cruciaal punt, mede ook gezien de gevolgen van nieuwe wetgeving op dit terrein met de Europese General Data Protection Regulation (GDPR).

Het beheersen van risico's komt met het gebruiken van een externe partij meer op afstand van de instelling te staan. Ook bij uitbesteding aan een gespecialiseerd RegTech-bedrijf, blijft de verantwoordelijkheid voor het beheersen van aan FEC gerelateerde risico's echter bij instellingen zelf. Wanneer het almaar wenselijker wordt geacht om technologie toe te passen, zullen instellingen zich moeten afvragen of dit ook niet tevens gepaard dient te gaan met de nodige investeringen om zelf kennis over technologische toepassingen in huis te hebben of om ten minste de technologie en de processen van de geboden oplossingen van RegTech-dienstverleners te begrijpen en te toetsen. Hierbij zullen tevens compliance en audit betrokken moeten zijn.

Daarnaast zullen vraagstukken aangaande verantwoordelijkheid en aansprakelijkheid met het gebruik van technologie de komende jaren steeds prominenter worden daar

waar instellingen er voor kiezen gezamenlijk op te trekken in het vergaren en delen van data. Vooral wanneer hierbij op termijn distributed ledger-technologie een rol zou gaan spelen en geen centrale partij meer de controle heeft, rijst de vraag wie verantwoordelijk is voor waarborgen omtrent de vergaring, kwaliteit en opslag van data en wanneer er bijvoorbeeld misbruik plaatsvindt door criminelen.

Vragen over verantwoordelijkheid en aansprakelijkheid spelen ook ten aanzien van kunstmatige intelligentie, zoals bijvoorbeeld toegepast in het hiervoor beschreven voorbeeld van transactiemonitoringsystemen. Het uitvoeren van transactiemonitoring met behulp van lerende algoritmes kan naast efficiëntie ook grote risico's met zich meebrengen. Bij een verkeerd algoritme, bijvoorbeeld een algoritme opgesteld met een bepaalde 'bias' waardoor ongebruikelijke transacties niet worden gedetecteerd ('false negatives'), zijn de gevolgen vele malen groter dan in een systeem zonder zelflerende algoritmes. De effectiviteit, functionaliteit en betrouwbaarheid van algoritmes zal constant aandacht vragen. Hierbij zal ook meer en meer de vraag naar voren komen hoe instellingen om zullen gaan met het veiligstellen van de integriteit van technologische toepassingen.

Waakzaamheid voor mogelijke onbedoelde neveneffecten zal van groot belang zijn bij de ontwikkelingen op het terrein van RegTech. Uit deze korte schets van mogelijke risico's, wordt in ieder geval evident dat mensen nodig blijven voor monitoring en daarmee mensen met kennis van technologische ontwikkelingen. De compliance officer zal hierbij binnen instellingen ook een essentiële rol vervullen door het stellen van kritische vragen en het fungeren als 'countervailing power' bij de ontwikkeling van nieuwe initiatieven.

5. Voorwaarden voor de toepassing van RegTech

Om de risico's rond het gebruiken van technologische oplossingen naar de toekomst toe zoveel mogelijk te beperken, kan er gedacht worden over een aantal voorwaarden waar aan moet worden voldaan alvorens de toepassing van RegTech kan plaatsvinden. Vanzelfsprekend zal voor instellingen voorop staan dat RegTech-oplossingen daadwerkelijk efficiënt zijn en zo veel mogelijk kostenbesparend in het voorkomen van betrokkenheid bij FEC. Daarnaast valt echter te denken aan een aantal andere elementen. Nieuwe technologieën zullen bijvoorbeeld uitgebreid getest moeten worden voordat deze worden ingebed in processen waarbij deze tests niet alleen zien op de effectiviteit, maar ook op het beperken van mogelijke onbedoelde neveneffecten van technologische toepassingen.

Gezien de eerder genoemde risico's bij het gebruiken van gespecialiseerde RegTech-dienstverleners, is due diligence op deze bedrijven in het bijzonder van belang alsmede het inregelen van zekerheden alvorens derde partijen worden ingeschakeld onder andere op het gebied van dataveiligheid. Een andere kernvoorwaarde voor het gebruiken van

RegTech-toepassingen, of deze nu door instellingen zelf worden ontwikkeld of door externe partijen, zal de transparantie zijn van de achterliggende technologie omtrent de keuzes die worden gemaakt in de ontwikkeling van RegTech-oplossingen. Instellingen zullen moeten waken over de integriteit van de door hun gebruikte technologie. Zo moet technologie dat doel dienen waar het ook voor is bedoeld.

Al met al gaat het gebruiken van technologie verder dan weten of het betrouwbaar is en werkt, het gaat ook over integriteit. In dit vroege stadium van verkenningen in de mogelijkheden van RegTech is daarom vereist dat medewerkers, waaronder compliance professionals, kennis hebben van technologie. Tevens zal op dit punt een belangrijke rol zijn weggelegd voor toezichthouders buiten instellingen zelf.

6. De rol van toezichthouders

Voor toezichthouders zijn vragen omtrent technologische ontwikkelingen minstens zo relevant als voor instellingen. Het landschap waarop toezichthouders toezien verandert van het type instellingen tot het type diensten en producten dat wordt geleverd. Bovendien krijgen ook toezichthouders steeds meer te maken met een datagedreven wereld waarin toezichthouden met behulp van technologische toepassingen eveneens van belang wordt. Hiervoor wordt ookwel de term 'suptech', supervisory technology, gebruikt. Als gevolg hiervan kijken ook toezichthouders met belangstelling naar de technologische ontwikkelingen die gaande zijn en mengen zich in discussies hierover.[9]

Als onderdeel van hun rol als toezichthouder geldt dat zij innovatieve ontwikkelingen op het terrein van technologie moeten volgen om te analyseren welke invloed deze zullen hebben op de sector. Op het terrein van FEC in het bijzonder, zullen toezichthouders zich op de hoogte moeten stellen van RegTech-ontwikkelingen bij instellingen gericht op een betere beheersing van aan FEC verbonden risico's. RegTech kan een belangrijk hulpmiddel zijn om naleving te bewerkstelligen, echter zoals in dit artikel kort belicht, zijn er ook de nodige risico's die met RegTech gepaard kunnen gaan. Toezicht zal zich op deze risico's moeten toespitsen en de mate waarin instellingen waarborgen dat RegTech niet alleen de efficiëntie verhoogd en kosten bespaard, maar ook de veiligheid, betrouwbaarheid, effectiviteit en integriteit van het financiële systeem niet schaadt.

Voor toezichthouders geldt tot slot ook dat zij belangrijke afwegingen dienen te maken in de wijze waarop ze in hun rol als toezichthouder gebruik maken van de steeds grotere hoeveelheid data die zij tot hun beschikking hebben en mogelijke technologie die zij

9 Zie bijvoorbeeld de activiteiten van de Financial Conduct Authority op dit terrein: www.fca.org.uk/firms/regtech.

daarbij kunnen gebruiken. Naast mogelijkheden om met meer datagedreven toezichtmethoden efficiënter toezicht te houden, brengt het gebruiken van meer data en technologische toepassingen in toezicht ook mogelijke aanvullende verantwoordelijkheden en risico's met zich mee. Toezichthouders zullen daarbij een zorgvuldige afweging dienen te maken over wat wenselijk is. De grens tussen toezicht en opsporing moet daarbij bewaakt worden, alsook de grens tussen waar verschillende toezichthouders verantwoordelijk voor zijn met meer inzichten verkregen uit data en individuele instellingen.

7. Conclusie

De mate waarin technologische ontwikkelingen impact zullen hebben op het terrein van de beheersing van risico's ten aanzien van FEC, zal de komende jaren steeds duidelijker worden. In dit artikel is een introductie geschetst van potentiele kansen en risico's op het terrein van RegTech in relatie tot het beheersen van aan FEC verbonden risico's. Hoewel de toepassing van RegTech in de bestrijding van FEC zich op dit moment nog in de beginfase bevindt, is de vraag niet zozeer of maar veel meer hoe en in welke mate RegTech een verschil zal kunnen maken in risicobeheersing en naleving. De invulling hiervan vergt betrokkenheid van zowel instellingen, externe partijen als toezichthouders om technologische oplossingen zo vorm te gegeven dat potentiele onbedoelde neveneffecten zoveel mogelijk gemitigeerd worden.