Voorkomen van witwassen en terrorismefinanciering is de beste aanpak

De beste aanpak van iedere criminaliteit, dus ook witwassen en terrorismefinanciering, is het voorkomen ervan. Toch zijn veel bestaande technieken reactief. Nieuwe technieken zoals het observeren van gedetailleerd klantgedrag maken een preventieve aanpak mogelijk, waardoor met minder kosten het risico op witwassen en terrorismefinanciering enorm verlaagd kan worden. Deze technieken worden al jaren succesvol ingezet bij fraudebestrijding, en het is dus niet meer dan logisch dit ook te doen ter voorkoming van witwassen en terrorismefinanciering. De laatste paar jaar wordt dit wereldwijd dan ook steeds meer gedaan.

De Engelse FCA heeft in een recente publicatie de waarde onderschreven van “behavioural biometrics”, oftewel biometrische gedragsgegevens. Dit om geldezels te herkennen en te voorkomen: https://www.fca.org.uk/publications/multi-firm-reviews/proceeds-fraud-detecting-preventing-money-mules. Voor de duidelijkheid: geldezels worden door criminelen niet alleen gebruikt om frauduleus verworven geld uit het bancaire systeem weg te sluizen, maar ook bij witwassen en dan met name bij placement en layering.

Toelichting op het voorkomen van geldezels

Het is efficiënter en effectiever om witwassen en terrorismefinanciering te voorkomen dan om te proberen het te herkennen als het al plaatsvindt. Voorkomen is een tweetrapsraket, waarvan de eerste trap is te zorgen dat de criminelen geen toegang krijgen tot bedrijf of instelling. Criminelen doen dit op verschillende manieren; allereerst door zelf klant te worden met eigen of gestolen gegevens. De bestaande clientacceptatie binnen het clientonderzoek richt zich op identificatie en accepteert de klant als deze klopt en de klantgegevens betrouwbaar zijn (of lijken). Dit kan veel effectiever: door het klantgedrag nauwkeurig te observeren is bijvoorbeeld te zien dat de klant zijn eigen naam en adres niet echt kent: hij gebruikt zijn kortetermijngeheugen in plaats van zijn langetermijngeheugen. Ook valt dan op dat de leeftijd op basis van gedrag niet overeenkomt met de opgegeven leeftijd. Aan de andere kant kent de crimineel het openingsproces een beetje te goed, en is erg vaardig met computers. Met deze en vele andere indicatoren zijn criminelen die klant worden met een hoge mate van precisie te herkennen. Ook als deze criminelen ervoor zorgen dat ze een laag-risicoklant lijken, en dus minder intensief gecontroleerd zullen worden.

De tweede trap is het herkennen van criminelen die op een andere manier zijn binnengekomen, en wel voordat ze daadwerkelijk actief kunnen worden. Die andere manieren om binnen te komen wordt het “oogsten” van rekeningen genoemd: door rekeningen van bestaande klanten over te nemen, nietsvermoedende klanten te overtuigen hun rekening te gebruiken voor administratief werk, of door al langer bestaande rekeningen te kopen, te lenen, of te hacken. Gebruikelijk is dat de voortdurende controle zich richt op transactiemonitoring, en dan natuurlijk ook andere dan betalingstransacties. Deze manier van detecteren is reactief: het herkent witwassen meestal pas als de betalingstransacties al gebeuren en dan zelden bij de eerste. Doordat criminelen zich heel anders gedragen dan echte klanten, zijn ze met een grote mate van zekerheid al te herkennen als ze rekeningen overnemen en klaarmaken voor gebruik. Door te focussen op het precieze gedrag kunnen crimineel gebruikte rekeningen veel eerder herkend worden, tot zelfs 6 maanden voordat de eerste criminele transactie binnenkomt.

Wereldwijde gegevens op basis van zo’n 50.000 via gedrag vroegtijdig gedetecteerde crimineel gebruikte bankrekeningen, laten zien dat circa 60% daarvan later voor witwassen en terrorismefinanciering gebruikt wordt, en de rest voor fraude. Deze cijfers laten ook zien dat circa

50% van deze rekeningen geopend wordt door criminelen, met eigen, gestolen, of nepgegevens, circa 40% wordt geoogst, en circa 10% wordt overgenomen door de rekening te hacken. Dit zijn cijfers over één jaar. Het blijkt ook mogelijk om gedetailleerd gedrag in te zetten om mensenhandel en moderne slavernij (HTMS) te herkennen.

Samenvoegen fraude-, witwas- en terrorismefinancieringsdetectie

Witwassen en terrorismefinanciering zijn efficiënter en effectiever te voorkomen en herkennen als sterk wordt samengewerkt met fraudedetectie, mogelijk zelfs samengevoegd.

Veel bedrijven en instellingen hebben de detectie van fraude en witwassen/terrorismefinanciering geoptimaliseerd, wat betekent dat ze apart ondergebracht zijn. Vaak nog wel in één Financial Economic Crime (FEC) sectie, maar dan in gescheiden afdelingen. Het is niet ongebruikelijk dat 2e-lijns witwasonderzoeken volledig worden afgeschermd van de rest van de organisatie, ook voor de fraudespecialisten.

Criminelen trekken zich niets aan van zulke interne scheidslijnen; ze maken er waar mogelijk juist gebruik van. In de criminele wereld heeft de afgelopen jaren een rationalisatie plaatsgevonden. Simpel voorbeeld hiervan zijn de rekeningen die gebruikt worden voor witwastransacties. Aparte groepen criminelen hebben zich gespecialiseerd op het aanmaken en oogsten van rekeningen, die vervolgens aan de hoogste bieder verkocht worden: zowel fraudeurs, als oplichters, als witwassers. Dit betekent dat als de detectie hiervan over verschillende afdelingen wordt verdeeld (Fraude en AML), dat dan per definitie ook de informatie nodig om dit te herkennen verdeeld wordt. En de mogelijkheden om het te herkennen kleiner worden. De oplossing hiervan is intensieve samenwerking tussen al deze afdelingen, en dit op alle gebieden: gegevens, technieken, middelen, procedures, medewerkers.

Samenvoegen fraude-, witwas- en terrorismefinancieringsdetectie (2)

Er is nog een reden om de detectie van fraude, witwassen en terrorismefinanciering samen te voegen. Alle soorten criminaliteit hebben gemeenschappelijk dat ze afwijken van gewoon gedrag, maar er zoveel mogelijk op proberen te lijken. Bedragen zijn afwijkend (hoger), en zijn meer betalingstransacties, ze kunnen op ongebruikelijke dagen en tijden plaatsvinden, etc. etc. Het is niet ongebruikelijk dat de eerste witwastransactie door de fraudeafdeling wordt opgemerkt, maar omdat de “klant” meldt deze transactie zelf gedaan te hebben en te willen doen, wordt de melding afgelegd als “geen fraude”. Dat klopt, maar het was wel witwassen en daarmee is een goede kans verkeken.

De huidige detectie richt zich primair op het vinden van bestaande fraude en witwaspatronen, wat de detectie per definitie reactief maakt. Het is extreem reactief om bij het ontdekken van een nieuw crimineel patroon een jaar terug te kijken of het al eerder heeft plaatsgevonden. Het is op zich begrijpelijk dat deze manier van detecteren wordt gebruikt, want het laat zich makkelijk vertalen in geautomatiseerde detectieregels en machine learning modellen getraind op bestaande fraude- of witwaspatronen. Het is echter ook mogelijk om detectiemodellen te maken die kijken naar afwijkend klantgedrag. Deze modellen herkennen zowel bestaand als nieuw crimineel gedrag en zijn daardoor niet of nauwelijks meer reactief. Deze modellen zijn zo te bouwen dat ze ook uitleg geven over de reden van het gegenereerde alarm, essentieel voor een goed onderzoek. Ook als er geen alarm gegeven wordt kan precies nagespeeld worden wat hiervoor de reden was, zodat het model verbeterd kan worden.

Het is intussen al in de praktijk aangetoond dat het gebruik van de juiste modellen het aantal verdachte transacties met 60% kan verhogen, terwijl het aantal foute alarmen met de helft verminderd kan worden.

Wiebe Fokma

Director - Global Advisory