

Zo voorspel je fraude bij online aankopen

08-11-2016 10:26



Door Chantal Rademaker de Ridder, director & consumer business industry lead en Johan ten Houten, senior manager financial crime analytics bij Deloitte Risk Advisory

Met Sinterklaas en Kerst in het verschiet maken online winkels zich op voor dé maand december. Met vier of vijf keer zoveel bestellingen als normaal is deze periode veruit de drukste tijd van het jaar. Naast het aantal retouren, bij sommige webshops wordt zo'n vijftig procent van de aankopen teruggestuurd, neemt in deze feestmaand het risico van niet betalende klanten en de kans op fraude eveneens explosief toe.

De Europese Bankenautoriteit (EBA), een van de financiële toezichthouders in Europa, pleit in dit verband voor een strengere authenticatie bij internetaankopen. Volgens de EBA zou de kans op fraude met digitaal betalen te groot zijn geworden.

Met de focus op omnichannel winkelen, het verrijken van de klantervaring en het vergemakkelijken van digitale betalingen zal dit een gebruikersvriendelijke en toegankelijke online betaalmethode moeten zijn. Het komt steeds vaker voor dat consumenten een aankoop offline of bijvoorbeeld op hun computer starten en de daadwerkelijke bestelling online of bijvoorbeeld met een app op de smartphone plaatsen. Een verplicht 'betaalkastje' voor alle internetaankopen boven de tien euro, zoals onlangs door [De Telegraaf](#) gemeld, is daarvoor te omslachtig. Een consument zou dan altijd het kastje bij zich moeten hebben om te kunnen betalen.

Smart analytics

Een oplossing die het gemak van online winkelen niet beperkt, en zelfs kan vergroten, is het inzetten van smart analytics. Bestellingen en aankoopgedrag kunnen daarmee worden geanalyseerd en de kans op het terugsturen van de bestelling, niet betalen of fraude worden voorspeld.

Wanneer je naar een bestelling zou kijken is het vaak eenvoudig te zien welke afwijkend is. Denk aan onevenredig veel bestellingen van één bepaald product op één adres. Welke consument bestelt er immers twee wasmachines en twee widescreen tv's tegelijk? Het handmatig bekijken van elke bestelling is echter te kostbaar en zou de doorlooptijd van de bestelling onnodig verlengen. Het maken van specifieke analyserregels om fraude te voorkomen – bijvoorbeeld wanneer op een huisadres in één keer meer dan drie identieke producten besteld worden blokkeer dan de bestelling – zal ook niet werken. Het bestellen van drie gelijke producten op zich is immers niet ongebruikelijk. En het duurt ook niet lang voordat een fraudeur doorheeft dat je wel drie wasmachines kunt bestellen maar dan drie verschillende types.

De oplossing is het gebruik maken van verschillende vormen van data-analyse technieken. In hoofdlijnen bieden twee soorten analyses uitkomst:

Ten eerste het gebruik van *predictive analytics*. Hierbij worden gegevens van nieuwe bestellingen vergeleken met een set van reeds eerder waargenomen fraudegevallen. Deze analyse maakt gebruik van analysetechnieken uit de kunstmatige intelligentie. De uitkomst van zo'n analyse – die in een paar milliseconden berekend wordt – geeft aan hoe waarschijnlijk de bestelling tegengehouden zou moet worden. Door het fraudeteam enkel naar deze voorbeelden te laten kijken is het mogelijk om vóór verzending een bestelling tegen te houden. Daarnaast levert het extra voorbeelden van fraudegevallen waardoor de analyse nog nauwkeuriger wordt. Aan het fraudeteam worden ook willekeurige voorbeelden aangeboden. Dit zouden mogelijk nieuwe voorbeelden zijn die het systeem nog niet herkent. Na beoordelen kunnen deze aan de bekende fraudegevallen worden toegevoegd.

Ten tweede *data pattern identification*. Deze analyse richt zich op afwijkingen en niet op voorbeelden. Voor elke klant is altijd wel een (bijna) vergelijkbare klant die in dezelfde situatie verkeert. Als de situatie vergelijkbaar is zal het bestelgedrag ook vergelijkbaar zijn. De analysetechniek bestaat eruit om groepen (de technische term is clusters) van bestellingen of klanten te maken en binnen een groep afwijkende bestellingen te onderzoeken. Ook deze voorbeelden kunnen na onderzoek worden gebruikt om de *predictive analytics* te voeden.

Door de beschikbare data rondom een bestelling goed en vooral tijdig in de gaten te houden is het mogelijk om actief fraude te bestrijden en zo schade door wanbetaling te voorkomen. Exact dezelfde technieken worden al met succes toegepast bij het controleren van pin- en creditcardbetalingen, het detecteren van verzekeringsfraude en bij diverse uitkeringsinstanties.