

MERCHANTS, PROVIDERS EN ISO'S

Transaction laundering: hoe providers het opsporen en hoe eerlijke merchants erin terechtkomen

Gepubliceerd op 28 september 2026

Betalingen van het ene bedrijf via het merchantaccount van een ander verwerken behoort tot de ernstigste overtredingen bij kaartbetalingen. Wat het is, hoe het wordt gevonden en welke gewone praktijken erop lijken.

Transaction laundering is het verwerken van de kaartbetalingen van het ene bedrijf via een merchantaccount dat voor een ander bedrijf is goedgekeurd. Het wordt ook factoring of ongeautoriseerde aggregatie genoemd. De accounthouder is door de risicobeoordeling gekomen. Het bedrijf dat het geld werkelijk ontvangt niet, en had dat meestal ook niet gekund.

Waarom het zo zwaar wordt opgenomen

Alles wat een betaaldienstverlener over risico weet, hangt aan de merchant die hij heeft goedgekeurd: wat die verkoopt, aan wie, voor welke prijs en met welke betwistingshistorie. Lopen de verkopen van een ander via dat account, dan klopt daar niets van. De provider draagt risico dat hij nooit heeft beoordeeld, en verplaatst mogelijk geld voor iets illegaals.

De kaartschema's houden de acquirer verantwoordelijk. Een zaak die een schema vindt, betekent boetes voor de acquirer, sluiting voor de merchant en meestal een vermelding op Mastercards MATCH-lijst onder de code voor laundering, waar maar heel weinig providers overheen stappen.

Hoe het wordt gevonden

Providers en de monitoringbedrijven die zij inschakelen, zoeken naar een kloof tussen waarvoor een account is goedgekeurd en wat het doet.

- **Websitemonitoring.** Crawlers controleren of de goedgekeurde site nog verkoopt wat hij verkocht, en zoeken naar andere sites die dezelfde checkout, dezelfde betaalpagina of dezelfde merchantkenmerken gebruiken.

- **Transactiepatronen.** Bedragen, tijdstippen en klantlanden die niet bij het goedgekeurde bedrijf passen. Een koffiewinkel ontvangt niet om drie uur 's nachts een reeks identieke ronde betalingen uit een ander continent.
- **Testaankopen.** Analisten kopen bij verdachte sites en kijken via welk merchantaccount de afschrijving binnenkomt.
- **De inhoud van betwistingen.** Een kaarthouder die een afschrijving betwist, zegt vaak wat hij werkelijk kocht. Is dat niet wat de merchant verkoopt, dan merkt de provider dat.
- **Verwijzer- en descriptorgegevens.** De pagina waar een klant vandaan kwam, en een descriptor op het afschrift die bij geen enkele goedgekeurde site past.

Hoe eerlijke merchants hetzelfde alarm laten afgaan

De meeste bedrijven die in deze controles terechtkomen, zijn nergens een dekmantel voor. Ze hebben iets gewoons gedaan zonder het hun provider te vertellen.

1. **Een tweede website op hetzelfde account.** Een nieuw merk of een nieuwe winkel, afgerekend via de bestaande checkout. Voor de monitoring is een niet-goedgekeurde site die via een goedgekeurd account betalingen aanneemt de definitie van het probleem.
2. **Een nieuwe productlijn.** Het account is goedgekeurd voor één soort goederen en verkoopt nu een andere, vooral een uit een beperkte categorie.
3. **Betalingen aannemen voor iemand anders.** Het bedrijf van een vriend, een leverancier, een zusterverenootschap. Dit is laundering in de letterlijke zin van de regels, wat de bedoeling ook is.
4. **Verkopen voor derden.** Een winkel die een marketplace wordt, verwerkt nu betalingen van andere verkopers, en daar hoort een ander soort account bij.
5. **Een gewijzigd bedrijfsmodel.** Overstappen van eenmalige verkopen naar abonnementen, of van goederen naar diensten, verandert het risico dat de provider heeft goedgekeurd.
6. **Affiliates en wederverkopers.** Partners die klanten naar pagina's sturen die de provider nooit heeft gezien.

Hoe u erbuiten blijft

- **Eén goedgekeurd bedrijf per account.** Zou u het tegenover een klant als een ander bedrijf beschrijven, dan heeft het een eigen goedkeuring nodig.
- **Meld het de provider voordat u iets verandert.** Nieuwe sites, producten, landen en factureringsmodellen. De meeste worden na een korte beoordeling goedgekeurd, en alle zien er veel slechter uit wanneer ze worden ontdekt.
- **Leen het account nooit uit.** Niet als gunst en niet tegen een vergoeding.
- **Houd de descriptor waarheidsgetrouw.** De naam op het afschrift moet terugleiden naar de site waar de klant kocht.

- **Weet wat uw partners doen.** Een merchant is aanspreekbaar op het verkeer dat zijn affiliates sturen.

Als een provider het aankaart

Antwoord snel en volledig. Leg uit wat de transacties waren, laat de betrokken sites zien en zeg wat er is veranderd. Een niet-gemelde tweede winkel die op de eerste dag wordt uitgelegd, is een compliancecorrectie. Dezelfde feiten die na een week stilte worden toegegeven, lijken op verhulling, en de provider moet ze zo behandelen.

Voor providers en ISO's

Het patroon achter de meeste echte gevallen is een aanvraag die net iets te schoon was: een eenvoudige winkel met laag risico, een nieuw domein, weinig verkeer en volume dat sneller binnenkomt dan de site kan verklaren. De gevallen die de meeste tijd kosten, zijn de eerlijke hierboven. Een vraag bij de onboarding naar andere sites, merken en geplande wijzigingen haalt er veel weg voordat ze beginnen.

Bronnen

- [LegitScript: de basis van BRAM en VIRP](#) (Engels)
- [Onlayer: wat transaction laundering is en hoe het wordt opgespoord](#) (Engels)

Online lezen: <https://payments-marketplace.com/nl-NL/insights/transaction-laundering/>

Payments Marketplace Ltd

Registered in England & Wales No. 17424288

Garden Ctg, Dereham Road, Dereham, Norfolk, NR19 2PW, UK

connect@payments-marketplace.com · +44 1366 727140