

MERCHANTS, PROVIDERS & ISOS

Transaction laundering: how providers detect it and how honest merchants get caught

Published 28 September 2026

Processing one business's payments through another's merchant account is among the most serious breaches in card payments. What it is, how it is found and the ordinary practices that look like it.

Transaction laundering is the processing of one business's card payments through a merchant account that was approved for a different business. It is also called factoring or unauthorised aggregation. The account holder passed underwriting. The business actually taking the money did not, and usually could not have.

Why it is treated so seriously

Everything a payment provider knows about risk is attached to the merchant it approved: what it sells, to whom, at what price and with what dispute history. When someone else's sales run through that account, none of it is true. The provider is carrying risk it never assessed, and may be moving money for something illegal.

The card schemes hold the acquirer responsible. A case found by a scheme brings fines for the acquirer, closure for the merchant and, usually, an entry on Mastercard's MATCH list under the code for laundering, which very few providers will look past.

How it is found

Providers and the monitoring firms they employ look for a gap between what an account was approved for and what it is doing.

- **Website monitoring.** Crawlers check that the approved site still sells what it did, and look for other sites using the same checkout, payment page or merchant identifiers.

- **Transaction patterns.** Amounts, times and customer countries that do not fit the approved business. A shop selling coffee does not take a run of identical round-number payments at three in the morning from another continent.
- **Test purchases.** Analysts buy from suspect sites and see which merchant account the charge arrives through.
- **Dispute content.** A cardholder disputing a charge often says what they actually bought. When that is not what the merchant sells, the provider notices.
- **Referrer and descriptor data.** The page a customer came from, and a statement descriptor that matches no site the provider approved.

How honest merchants trip the same alarms

Most businesses caught by these controls are not fronts for anything. They did something ordinary without telling their provider.

1. **A second website on the same account.** A new brand or a new shop, paid through the existing checkout. To monitoring, an unapproved site taking payments on an approved account is the definition of the problem.
2. **A new product line.** The account was approved for one kind of goods and now sells another, particularly one in a restricted category.
3. **Taking payments for someone else.** A friend's business, a supplier, a sister company. This is laundering in the plain sense of the rules, whatever the intention.
4. **Selling for third parties.** A shop that becomes a marketplace is now handling other sellers' payments, which needs a different kind of account.
5. **A changed business model.** Moving from one-off sales to subscriptions, or from goods to services, changes the risk the provider approved.
6. **Affiliates and resellers.** Partners who send customers to pages the provider has never seen.

Staying clear of it

- **One approved business per account.** If you would describe it to a customer as a different business, it needs its own approval.
- **Tell the provider before you change.** New sites, products, countries and billing models. Most are approved with a short review, and all of them look far worse when discovered.
- **Never lend the account.** Not as a favour and not for a fee.
- **Keep the descriptor true.** The name on the statement should lead back to the site the customer bought from.
- **Know what your partners are doing.** A merchant is answerable for the traffic its affiliates send.

If a provider raises it

Answer quickly and completely. Explain what the transactions were, show the sites involved and say what has been changed. An undeclared second shop explained on the first day is a compliance correction. The same facts admitted after a week of silence look like concealment, and the provider has to treat them that way.

For providers and ISOs

The pattern behind most genuine cases is an application that was a little too clean: a simple low-risk shop, a new domain, little traffic and volume that arrives faster than the site could explain. The cases that waste the most time are the honest ones above. A question at onboarding about other sites, brands and planned changes removes many of them before they start.

Sources

- [LegitScript: BRAM and VIRP basics](#)
- [Onlayer: what transaction laundering is and how it is detected](#)

Read online: <https://payments-marketplace.com/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