

MARCHANDS, PRESTATAIRES ET ISO

# Blanchiment de transactions : comment les prestataires le détectent et comment des marchands honnêtes se font prendre

Publié le 28 septembre 2026

Traiter les paiements d'une entreprise par le compte marchand d'une autre est l'un des manquements les plus graves dans les paiements par carte. Ce que c'est, comment on le découvre et les pratiques ordinaires qui y ressemblent.

Le blanchiment de transactions, ou transaction laundering, consiste à traiter les paiements par carte d'une entreprise par un compte marchand qui a été approuvé pour une autre. On parle aussi de factoring ou d'agrégation non autorisée. Le titulaire du compte a passé l'analyse des risques. L'entreprise qui encaisse réellement l'argent ne l'a pas passée et, le plus souvent, n'aurait pas pu.

## Pourquoi c'est pris si au sérieux

Tout ce qu'un prestataire de paiement sait du risque est attaché au marchand qu'il a approuvé : ce qu'il vend, à qui, à quel prix et avec quel historique de contestations. Quand les ventes d'un autre passent par ce compte, rien de tout cela n'est vrai. Le prestataire porte un risque qu'il n'a jamais évalué, et fait peut-être circuler de l'argent pour quelque chose d'illégal.

Les réseaux de cartes tiennent l'acquéreur pour responsable. Un cas découvert par un réseau entraîne des amendes pour l'acquéreur, la fermeture pour le marchand et, généralement, une inscription sur la liste MATCH de Mastercard sous le code de blanchiment, sur lequel très peu de prestataires passeront.

## Comment on le découvre

Les prestataires et les sociétés de surveillance qu'ils emploient cherchent un écart entre ce pour quoi un compte a été approuvé et ce qu'il fait.

- **La surveillance du site web.** Des robots vérifient que le site approuvé vend toujours la même chose et cherchent d'autres sites utilisant le même checkout, la même page de paiement ou les mêmes identifiants marchands.

- **Les schémas de transactions.** Des montants, des horaires et des pays de clients qui ne correspondent pas à l'activité approuvée. Une boutique de café n'encaisse pas à trois heures du matin une série de paiements identiques de montant rond venus d'un autre continent.
- **Les achats tests.** Des analystes achètent sur des sites suspects et regardent par quel compte marchand le débit arrive.
- **Le contenu des contestations.** Un porteur qui conteste un débit dit souvent ce qu'il a réellement acheté. Quand ce n'est pas ce que vend le marchand, le prestataire le remarque.
- **Les données de provenance et de libellé.** La page d'où venait le client, et un libellé de relevé qui ne correspond à aucun site approuvé par le prestataire.

## Comment des marchands honnêtes déclenchent les mêmes alertes

La plupart des entreprises prises par ces contrôles ne servent de façade à rien. Elles ont fait quelque chose d'ordinaire sans le dire à leur prestataire.

1. **Un second site web sur le même compte.** Une nouvelle marque ou une nouvelle boutique, encaissée par le checkout existant. Pour la surveillance, un site non approuvé qui encaisse sur un compte approuvé est la définition même du problème.
2. **Une nouvelle gamme de produits.** Le compte a été approuvé pour un type de biens et en vend désormais un autre, en particulier dans une catégorie restreinte.
3. **Encaisser pour quelqu'un d'autre.** L'entreprise d'un ami, d'un fournisseur, d'une société sœur. C'est du blanchiment au sens littéral des règles, quelle que soit l'intention.
4. **Vendre pour des tiers.** Une boutique qui devient marketplace gère désormais les paiements d'autres vendeurs, ce qui exige un autre type de compte.
5. **Un modèle économique modifié.** Passer de ventes ponctuelles à des abonnements, ou de biens à des services, modifie le risque que le prestataire a approuvé.
6. **Les affiliés et les revendeurs.** Des partenaires qui envoient des clients vers des pages que le prestataire n'a jamais vues.

## Comment s'en tenir à l'écart

- **Une activité approuvée par compte.** Si vous la décririez à un client comme une autre entreprise, elle a besoin de sa propre approbation.
- **Prévenez le prestataire avant de changer.** Nouveaux sites, produits, pays et modes de facturation. La plupart sont approuvés après un bref examen, et tous paraissent bien pires une fois découverts.
- **Ne prêtez jamais le compte.** Ni par service rendu, ni contre rémunération.
- **Gardez un libellé exact.** Le nom sur le relevé doit ramener au site sur lequel le client a acheté.
- **Sachez ce que font vos partenaires.** Un marchand répond du trafic que lui envoient ses affiliés.

## Si un prestataire soulève la question

Répondez vite et complètement. Expliquez ce qu'étaient les transactions, montrez les sites concernés et dites ce qui a été modifié. Une seconde boutique non déclarée, expliquée dès le premier jour, est une correction de conformité. Les mêmes faits reconnus après une semaine de silence ressemblent à une dissimulation, et le prestataire doit les traiter comme telle.

## Pour les prestataires et les ISO

Le schéma derrière la plupart des cas réels est une demande un peu trop propre : une boutique simple à faible risque, un nom de domaine récent, peu de trafic et un volume qui arrive plus vite que le site ne peut l'expliquer. Les cas qui font perdre le plus de temps sont les cas honnêtes ci-dessus. Une question à l'entrée en relation sur les autres sites, les autres marques et les changements prévus en élimine beaucoup avant qu'ils ne commencent.

## Sources

- [LegitScript : les bases de BRAM et de VIRP](#) (en anglais)
- [Onlayer : ce qu'est le blanchiment de transactions et comment il est détecté](#) (en anglais)

---

Lire en ligne : <https://payments-marketplace.com/fr-FR/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](mailto:connect@payments-marketplace.com) · +44 1366 727140