

COMERCIOS, PROVEEDORES E ISO

Blanqueo de operaciones: cómo lo detectan los proveedores y cómo caen en él los comercios honrados

Publicado el 28 de septiembre de 2026

Procesar los pagos de un negocio a través de la cuenta de comercio de otro es una de las infracciones más graves en los pagos con tarjeta. Qué es, cómo se descubre y las prácticas corrientes que se le parecen.

El blanqueo de operaciones, o transaction laundering, consiste en procesar los pagos con tarjeta de un negocio a través de una cuenta de comercio aprobada para un negocio distinto. También se llama factoring o agregación no autorizada. El titular de la cuenta superó el análisis de riesgo. El negocio que realmente cobra no lo superó y, por lo general, no habría podido.

Por qué se trata con tanta seriedad

Todo lo que un proveedor de pagos sabe del riesgo va unido al comercio que aprobó: qué vende, a quién, a qué precio y con qué historial de disputas. Cuando las ventas de otro pasan por esa cuenta, nada de eso es cierto. El proveedor asume un riesgo que nunca evaluó, y puede estar moviendo dinero de algo ilegal.

Las marcas de tarjetas hacen responsable al adquirente. Un caso detectado por una marca supone multas para el adquirente, el cierre para el comercio y, normalmente, una anotación en la lista MATCH de Mastercard con el código de blanqueo, que muy pocos proveedores pasan por alto.

Cómo se descubre

Los proveedores y las empresas de seguimiento que contratan buscan una brecha entre aquello para lo que se aprobó una cuenta y lo que está haciendo.

- **Seguimiento del sitio web.** Los rastreadores comprueban que el sitio aprobado sigue vendiendo lo mismo, y buscan otros sitios que usen el mismo checkout, la misma página de pago o los mismos identificadores de comercio.

- **Patrones de operaciones.** Importes, horas y países de los clientes que no encajan con el negocio aprobado. Una tienda de café no recibe una serie de pagos idénticos de importe redondo a las tres de la madrugada desde otro continente.
- **Compras de prueba.** Los analistas compran en sitios sospechosos y ven por qué cuenta de comercio llega el cargo.
- **El contenido de las disputas.** El titular que disputa un cargo suele decir qué compró en realidad. Cuando eso no es lo que vende el comercio, el proveedor lo nota.
- **Datos de procedencia y de descriptor.** La página desde la que llegó el cliente, y un descriptor en el extracto que no corresponde a ningún sitio aprobado por el proveedor.

Cómo activan las mismas alarmas los comercios honrados

La mayoría de los negocios atrapados por estos controles no son tapadera de nada. Hicieron algo corriente sin decírselo a su proveedor.

1. **Un segundo sitio web en la misma cuenta.** Una marca nueva o una tienda nueva, cobrada a través del checkout existente. Para el seguimiento, un sitio no aprobado que cobra por una cuenta aprobada es la definición del problema.
2. **Una nueva línea de productos.** La cuenta se aprobó para un tipo de producto y ahora vende otro, sobre todo si es de una categoría restringida.
3. **Cobrar por cuenta de otro.** El negocio de un amigo, de un proveedor, de una sociedad hermana. Esto es blanqueo en el sentido literal de las normas, sea cual sea la intención.
4. **Vender para terceros.** Una tienda que se convierte en marketplace gestiona ahora los pagos de otros vendedores, lo que requiere otro tipo de cuenta.
5. **Un modelo de negocio distinto.** Pasar de ventas únicas a suscripciones, o de productos a servicios, cambia el riesgo que el proveedor aprobó.
6. **Afiliados y revendedores.** Socios que envían clientes a páginas que el proveedor nunca ha visto.

Cómo mantenerse al margen

- **Un negocio aprobado por cuenta.** Si se lo describiría a un cliente como un negocio distinto, necesita su propia aprobación.
- **Avise al proveedor antes de cambiar.** Sitios, productos, países y modelos de cobro nuevos. La mayoría se aprueba con una revisión breve, y todos parecen mucho peores cuando se descubren.
- **No preste nunca la cuenta.** Ni como favor ni a cambio de una comisión.
- **Mantenga veraz el descriptor.** El nombre del extracto debe llevar al sitio en el que compró el cliente.
- **Sepa lo que hacen sus socios.** El comercio responde del tráfico que envían sus afiliados.

Si un proveedor lo plantea

Responda rápido y por completo. Explique qué eran las operaciones, muestre los sitios implicados y diga qué se ha cambiado. Una segunda tienda no declarada y explicada el primer día es una corrección de cumplimiento. Los mismos hechos admitidos tras una semana de silencio parecen ocultación, y el proveedor tiene que tratarlos así.

Para proveedores e ISO

El patrón que hay detrás de la mayoría de los casos reales es una solicitud un poco demasiado limpia: una tienda sencilla de bajo riesgo, un dominio nuevo, poco tráfico y un volumen que llega más deprisa de lo que el sitio podría explicar. Los casos que más tiempo hacen perder son los honrados de arriba. Una pregunta en el alta sobre otros sitios, marcas y cambios previstos elimina muchos antes de que empiecen.

Fuentes

- [LegitScript: conceptos básicos de BRAM y VIRP](#) (en inglés)
- [Onlayer: qué es el blanqueo de operaciones y cómo se detecta](#) (en inglés)

Leer en línea: <https://payments-marketplace.com/es-ES/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