

HÄNDLER, ANBIETER UND ISOS

Transaction Laundering: Wie Anbieter es erkennen und wie ehrliche Händler hineingeraten

Veröffentlicht am 28. September 2026

Zahlungen eines Unternehmens über das Händlerkonto eines anderen abzuwickeln gehört zu den schwersten Verstößen im Kartengeschäft. Was es ist, wie es auffällt und welche gewöhnlichen Praktiken danach aussehen.

Transaction Laundering ist die Abwicklung der Kartenzahlungen eines Unternehmens über ein Händlerkonto, das für ein anderes Unternehmen genehmigt wurde. Man spricht auch von Factoring oder unerlaubter Aggregation. Der Kontoinhaber hat die Risikoprüfung bestanden. Das Unternehmen, das tatsächlich das Geld einnimmt, hat es nicht und hätte es meist auch nicht gekonnt.

Warum es so ernst genommen wird

Alles, was ein Zahlungsanbieter über das Risiko weiß, hängt an dem Händler, den er genehmigt hat: was er verkauft, an wen, zu welchem Preis und mit welcher Streitfallhistorie. Laufen die Umsätze eines anderen über dieses Konto, stimmt nichts davon. Der Anbieter trägt ein Risiko, das er nie bewertet hat, und bewegt womöglich Geld für etwas Illegales.

Die Kartenorganisationen machen den Acquirer verantwortlich. Ein von einer Kartenorganisation entdeckter Fall bringt dem Acquirer Strafen, dem Händler die Schließung und meist einen Eintrag in Mastercards MATCH-Liste unter dem Code für Laundering, über den nur sehr wenige Anbieter hinwegsehen.

Wie es auffällt

Anbieter und die von ihnen beauftragten Monitoring-Firmen suchen nach einer Lücke zwischen dem, wofür ein Konto genehmigt wurde, und dem, was es tut.

- **Website-Monitoring.** Crawler prüfen, ob die genehmigte Website noch verkauft, was sie verkaufte, und suchen nach anderen Websites, die denselben Checkout, dieselbe Zahlungsseite

oder dieselben Händlerkennungen nutzen.

- **Transaktionsmuster.** Beträge, Uhrzeiten und Kundenländer, die nicht zum genehmigten Geschäft passen. Ein Kaffeeladen nimmt nicht um drei Uhr nachts eine Serie identischer runder Zahlungen von einem anderen Kontinent ein.
- **Testkäufe.** Analysten kaufen auf verdächtigen Websites und sehen, über welches Händlerkonto die Belastung eintrifft.
- **Inhalte von Streitfällen.** Ein Karteninhaber, der eine Belastung bestreitet, sagt oft, was er tatsächlich gekauft hat. Wenn der Händler das nicht verkauft, bemerkt es der Anbieter.
- **Referrer- und Deskriptor-Daten.** Die Seite, von der ein Kunde kam, und ein Deskriptor auf dem Kontoauszug, der zu keiner genehmigten Website passt.

Wie ehrliche Händler dieselben Alarme auslösen

Die meisten Unternehmen, die in diese Kontrollen geraten, sind keine Tarnung für irgendetwas. Sie haben etwas Gewöhnliches getan, ohne es ihrem Anbieter zu sagen.

1. **Eine zweite Website auf demselben Konto.** Eine neue Marke oder ein neuer Shop, bezahlt über den bestehenden Checkout. Für das Monitoring ist eine nicht genehmigte Website, die über ein genehmigtes Konto Zahlungen annimmt, die Definition des Problems.
2. **Eine neue Produktlinie.** Das Konto wurde für eine Warenart genehmigt und verkauft nun eine andere, besonders eine aus einer beschränkten Kategorie.
3. **Zahlungen für jemand anderen annehmen.** Das Geschäft eines Freundes, eines Lieferanten, einer Schwestergesellschaft. Das ist Laundering im schlichten Sinn der Regeln, gleich mit welcher Absicht.
4. **Verkauf für Dritte.** Ein Shop, der zum Marktplatz wird, wickelt nun Zahlungen anderer Verkäufer ab, und das erfordert eine andere Art von Konto.
5. **Ein geändertes Geschäftsmodell.** Der Wechsel von Einzelverkäufen zu Abonnements oder von Waren zu Dienstleistungen verändert das Risiko, das der Anbieter genehmigt hat.
6. **Affiliates und Wiederverkäufer.** Partner, die Kunden auf Seiten schicken, die der Anbieter nie gesehen hat.

Wie Sie sich davon fernhalten

- **Ein genehmigtes Geschäft je Konto.** Würden Sie es einem Kunden als ein anderes Geschäft beschreiben, braucht es eine eigene Genehmigung.
- **Informieren Sie den Anbieter, bevor Sie etwas ändern.** Neue Websites, Produkte, Länder und Abrechnungsmodelle. Das meiste wird nach kurzer Prüfung genehmigt, und alles sieht weit schlimmer aus, wenn es entdeckt wird.
- **Verleihen Sie das Konto nie.** Nicht aus Gefälligkeit und nicht gegen Entgelt.

- **Halten Sie den Deskriptor wahr.** Der Name auf dem Kontoauszug sollte zu der Website zurückführen, auf der der Kunde gekauft hat.
- **Wissen Sie, was Ihre Partner tun.** Ein Händler ist für den Traffic verantwortlich, den seine Affiliates schicken.

Wenn ein Anbieter es anspricht

Antworten Sie schnell und vollständig. Erklären Sie, worum es bei den Transaktionen ging, zeigen Sie die beteiligten Websites und sagen Sie, was geändert wurde. Ein nicht gemeldeter zweiter Shop, am ersten Tag erklärt, ist eine Compliance-Korrektur. Dieselben Tatsachen, nach einer Woche Schweigen eingeräumt, sehen nach Verschleierung aus, und der Anbieter muss sie so behandeln.

Für Anbieter und ISOs

Das Muster hinter den meisten echten Fällen ist ein Antrag, der etwas zu sauber war: ein einfacher risikoarmer Shop, eine neue Domain, wenig Traffic und Volumen, das schneller kommt, als die Website erklären könnte. Am meisten Zeit kosten die ehrlichen Fälle oben. Eine Frage beim Onboarding nach weiteren Websites, Marken und geplanten Änderungen räumt viele davon aus, bevor sie entstehen.

Quellen

- [LegitScript: Grundlagen zu BRAM und VIRP](#) (Englisch)
- [Onlayer: Was Transaction Laundering ist und wie es erkannt wird](#) (Englisch)

Online lesen: <https://payments-marketplace.com/de-DE/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