Solution Brief

Transaction Laundering Detection

Prevent card network scrutiny and reduce chargebacks with multifaceted fraud detection.

The threat of transaction laundering — unknowingly processing payments on behalf of a business you never approved — plagues even the savviest of payment providers. An ill-intentioned merchant creates a seemingly innocuous website and uses it to process transactions for **prohibited or illegal goods**. With developments in AI, fraudsters are:

1. Capitalizing on how easily and quickly they can start an online shop.
2. Creating websites and merchant accounts at higher volumes than ever before.
3. Becoming increasingly difficult to detect.

Effective detection requires a multifaceted approach that scrutinizes the merchant from all angles and uses cutting-edge technology for good. Only LegitScript's detection is so thorough.

Transaction Laundering Threatens Your Relationships, Your Reputation, and Your Bottom Line

Hard to spot but impossible to ignore, ramifications can be severe and include:

Card Network Scrutiny	Transaction laundering is among the highest concerns for major card networks, especially if it is being used to process payments for high-risk categories such as illegal pharmaceuticals, psychoactive products, gambling, and illegal adult content.
Fines	Card network scrutiny can yield expensive assessments and cause long-term damage to relationships with networks and acquirers.
Increased Chargebacks	Transaction laundering can result in increased chargebacks, especially as transaction laundering is increasingly used for fraud such as non-delivery schemes.
Reputational Harm	Customers harmed by fraud or dangerous products can draw negative press and bad reviews, and strain industry relationships.

LegitScript

Our approach combines risk data across the internet, AI-driven detection and insights, and our investigative analysts' expert insights to stop transaction launderers at every turn.

Case Study: How We Uncover Transaction Laundering

Merchant website scrutiny is a critical first step. For example, a handbag website (below on left) appears legitimate at first glance, but LegitScript analysts spotted red flags that prompted us to dig deeper, revealing a rogue internet pharmacy.

Merchant Website

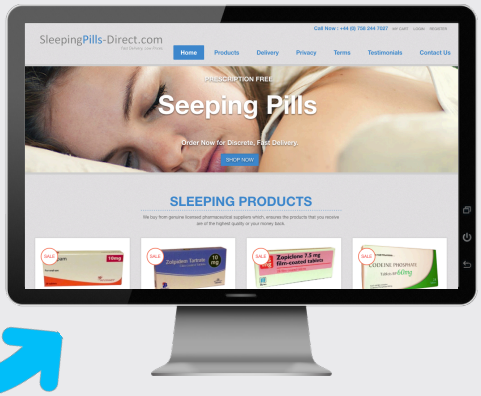
Fake Handbags Business

Problems with the merchant website:

- An incongruous domain name
- A generic template with stock images
- Odd, generic product descriptions
- Typos and inconsistent pricing

Real Operation

Illicit Drugs Website



Further investigation by LegitScript's transaction laundering experts revealed that the merchant website was a front business that was processing payments for illicit prescription sleeping pills.

We Go Beyond the Provided Website to Root Out Fraud

LegitScript performs **in-depth investigations** and **network mapping** to find indications and evidence of transaction laundering, connecting the dots to detect repeat offenders and turn suspicions into actionable proof. Our process includes:

- **Test Transactions.** Our dedicated team of transaction laundering experts performs test purchases to learn about an operation and gather important evidence such as a mismatched merchant descriptor.
- **DNS and Business Registration Research.** We look at domain name system (DNS) information, such as IP addresses and other technical data, and business registration records to evaluate connections to other websites and entities.
- **Internet Presence.** Our team searches social media and online reviews to assess the internet presence and see if customers have posted about scams, suspicious charges, or other problematic behavior.
- **Nuanced Insights.** We summarize and categorize findings, distinguishing suspected and confirmed transaction laundering for your streamlined action.

LegitScript: Making the Internet and Payment Ecosystems Safer and More Transparent – Now and for Future Generations

Contact Us
legitscript.com/contact

PGE-GE193-FSE-02