# Zombie Transaction Launderers

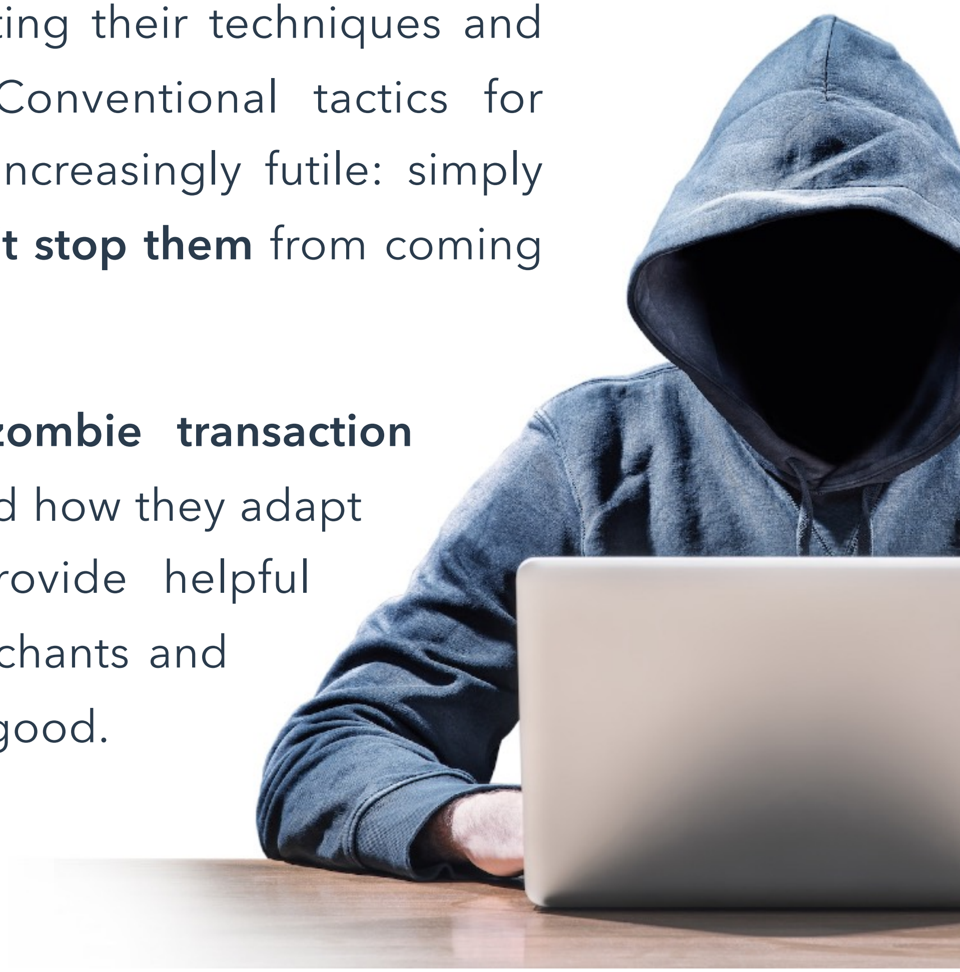
## How to Stop Reoffending TL Merchants That Won't Die

LegitScript

# Introduction

Among the most pervasive pain points for acquirers and payment service providers (PSPs) are **transaction launderers**, who have become masters at adapting their techniques and approaches to evade detection. Conventional tactics for tackling transaction launderers are increasingly futile: simply shutting down these merchants **won't stop them** from coming back in more dangerous forms.

In this report, we explain what **zombie transaction launderers** are, how they operate, and how they adapt to monitoring efforts. We also provide helpful tactics on how to identify these merchants and remove them from your portfolio for good.



# Zombie Transaction Launderers

## Report

# 1 What is a Zombie Transaction Launderer?

Transaction launderers are nothing if not persistent. Once terminated, they often attempt to re-ingest themselves repeatedly into portfolios with the same domain name, or sometimes even multiple other domain names. LegitScript defines these persistent rogue merchants as "zombie transaction launderers" because, simply put, **they just won't die**.

Compounding the problem, these serial transaction launderers are known to advertise their services to **multiple criminal networks**, reinforcing the incentive to continually assail payment service providers and probe for blind spots in their detection methods.

Helpful Resources

What is Transaction Laundering?

# 2 What's Inside the Zombie Transaction Launderer's Toolbox

With each successive iteration of their submitted merchant applications, zombie transaction laundering merchants often develop **better discernment** for what provokes termination from their acquirer. As a result, subsequent fraudulent accounts become **more difficult to identify**.

Initially, the changes in the merchant application are typically perfunctory. Common strategies include changing the top-level domain of a website, altering only one field of the necessary merchant application information, or even just adopting a new Merchant Category Code. However, once these methods fail, some of the more insistent offenders will employ **sophisticated obfuscation tactics**, including using fake names, partnering with legitimate domain names by promising a kickback, or, in extreme cases, emulating the content of small, legitimate websites and impersonating their unsuspecting operators as a method of camouflage.

# 3 When Payment Service Providers Fail in Their Detection Efforts

Many PSPs take a piecemeal approach to cracking down on TL websites, which is an insufficient method that can lead to **card issuer fines** or even **government intervention**. Removing TL merchants individually as they sprout up is like pulling a weed without addressing the problematic root system below.

In addition to the risk of punitive action, there are several other practical reasons why acquirers need to be more diligent in tackling zombie transaction launderers. One of these is the existing **communication networks** within laundering circles. While some transaction launderers operate in a vacuum, many of them belong to groups whose purpose is to exchange information on strategies and targets. These **laundering circles** are keen to discover weaknesses in PSPs and identify easy marks for illicit activity.

A diligent payment service provider is unlikely to become a target for these transaction laundering circles if it swiftly addresses TL merchants and utilizes a variety of countermeasures to combat reoffenders. More complex e-commerce laundering schemes are arduous, require specialized skills to implement, and often cost transaction launderers more upfront. Criminals will tend to stick with the **easier targets**.

Helpful Resources

Anatomy of a Transaction Launderer

# 4 Why TL Merchants Use Multiple Payment Service Providers

Besides re-ingesting with altered merchant record details, transaction launderers often **migrate between payment service providers**. When simple efforts to breach one provider continue to fail, moving to another can be the most practical of available options.

However, even if zombie transaction launderers succeed in avoiding detection by an acquirer, they often ingest into multiple portfolios as a method of **load balancing**, ensuring minimal disruption if termination occurs. It's important for payment service providers to know that transaction laundering merchants will typically attempt to **persist in their portfolios** to help provide the necessary insurance against service disruption. This is one of the reasons zombie transaction launderers keep coming back.

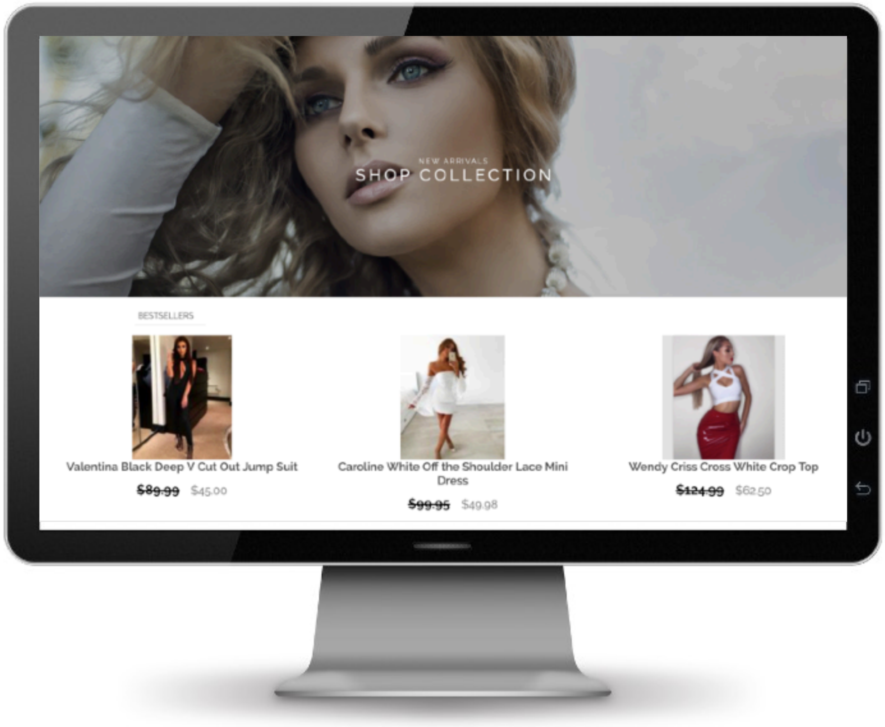
# 5 How to Make Zombie Transaction Launderers Unwelcome

There is no silver bullet guaranteeing transaction launderers will not reoffend. Aggressive compliance policies do, however, drastically reduce the likelihood. It is not enough to shut off single violative merchant accounts. When a transaction laundering merchant is uncovered, payment service providers should **initiate sweeps of their portfolios** to locate related merchant accounts and terminate the entire cluster.

Following these terminations, successful management of zombie TL merchants includes monitoring that **parses incoming applications** for similar record data. Useful merchant fields for tracking include merchant names, merchant descriptors, IP addresses from which merchant accounts are managed, contact information, and legal business names. If your company does not have the technical capability to do this, LegitScript offers **expert monitoring solutions**.

# Case Study: A Zombie TL Merchant Reveals a Laundering Cluster

In late 2018, LegitScript encountered a clothing website exhibiting several **transaction laundering characteristics**, including odd pricing, a lack of significant web presence, and mismatching merchant record data.

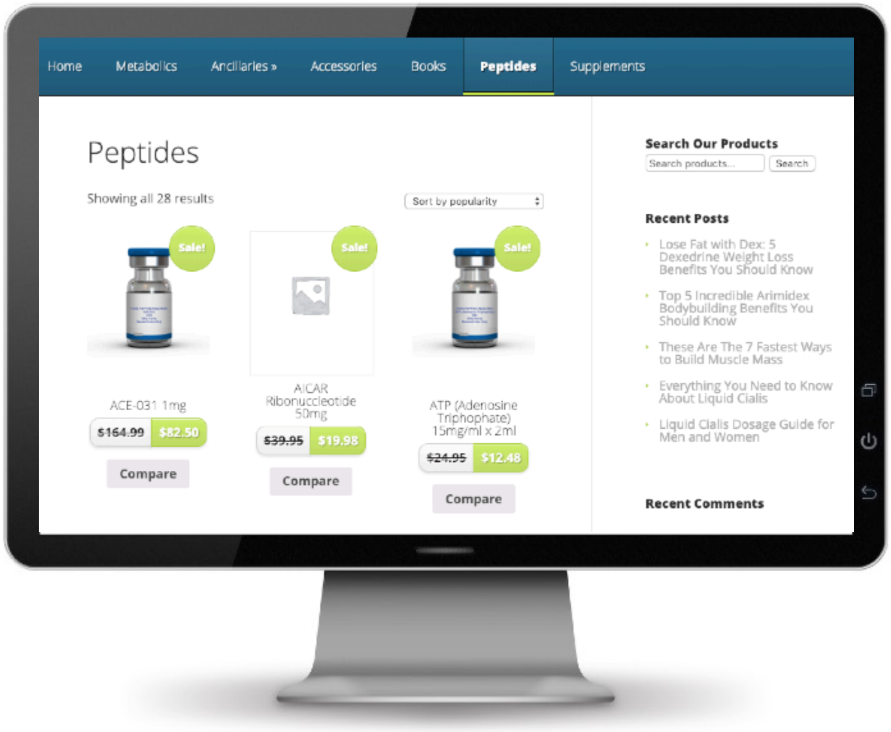


Valentina Black Deep V Cut Out Jump Suit
~~$89.99~~ $45.00

Caroline White Off the Shoulder Lace Mini Dress
~~$99.95~~ $49.98

Wendy Criss Cross White Crop Top
~~$124.99~~ $62.50

Using the merchant descriptor, a relatively straightforward connection was established to a website illegally offering **peptides** and **protein-based drugs** that are not approved in the US for any indication. LegitScript reported the account, resulting in immediate termination.



Peptides

Showing all 28 results

ACE-031 1mg
~~$164.99~~ $82.50

AICAR Ribonuccleotide 50mg
~~$39.95~~ $19.98

ATP (Adenosine Triphophate) 15mg/ml x 2ml
~~$24.95~~ $12.48

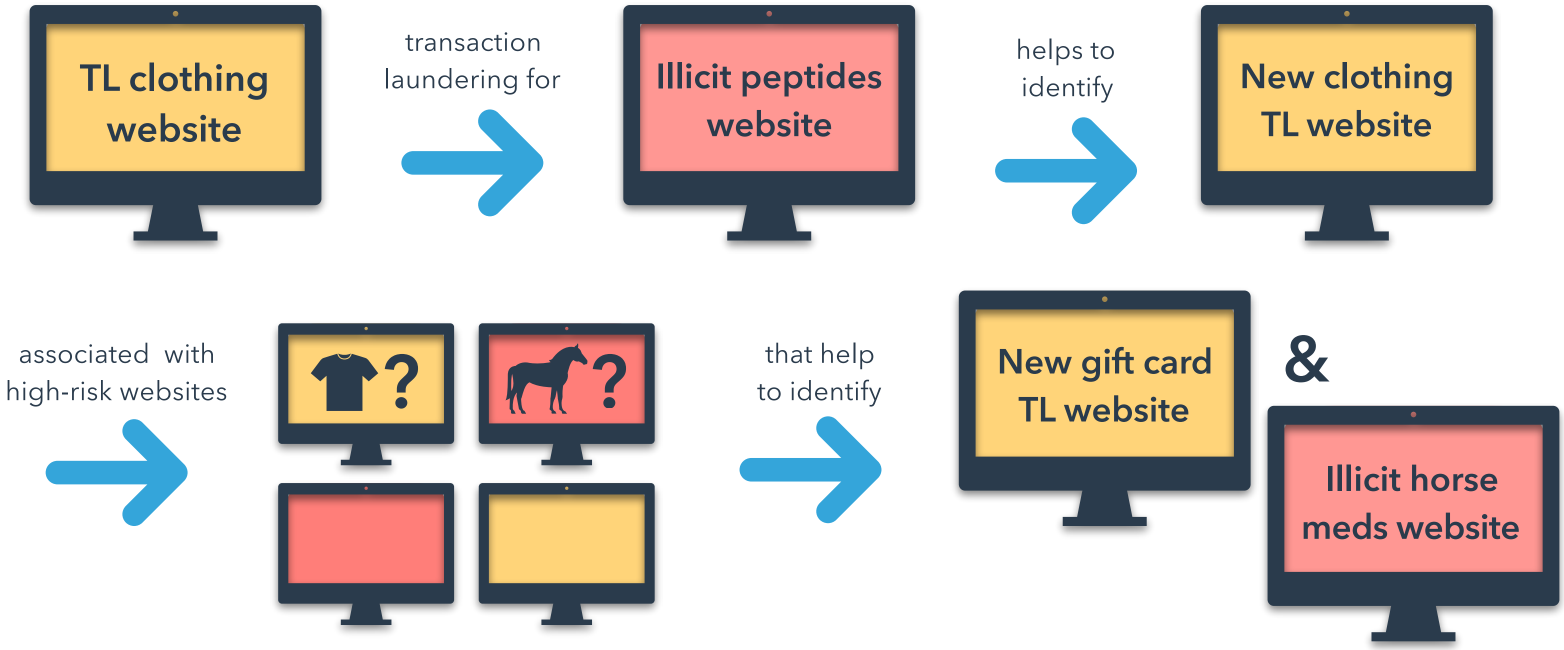
Search Our Products

Recent Posts

- Lose Fat with Dex: 5 Dexedrine Weight Loss Benefits You Should Know
- Top 5 Incredible Arimidex Bodybuilding Benefits You Should Know
- These Are The 7 Fastest Ways to Build Muscle Mass
- Everything You Need to Know About Liquid Cialis
- Liquid Cialis Dosage Guide for Men and Women

Recent Comments

One week later, the merchant returned with the clothing store website using a **different merchant descriptor**, presumably having learned the error of utilizing the peptides business' operating name in record data. The merchant was again immediately terminated and reported, and LegitScript investigated further to identify other **affiliated accounts**. Our analysts identified one account using a business name redolent of the clothing store, and another featuring a name suggesting involvement in facilitating the sale of **equine pharmaceuticals**.



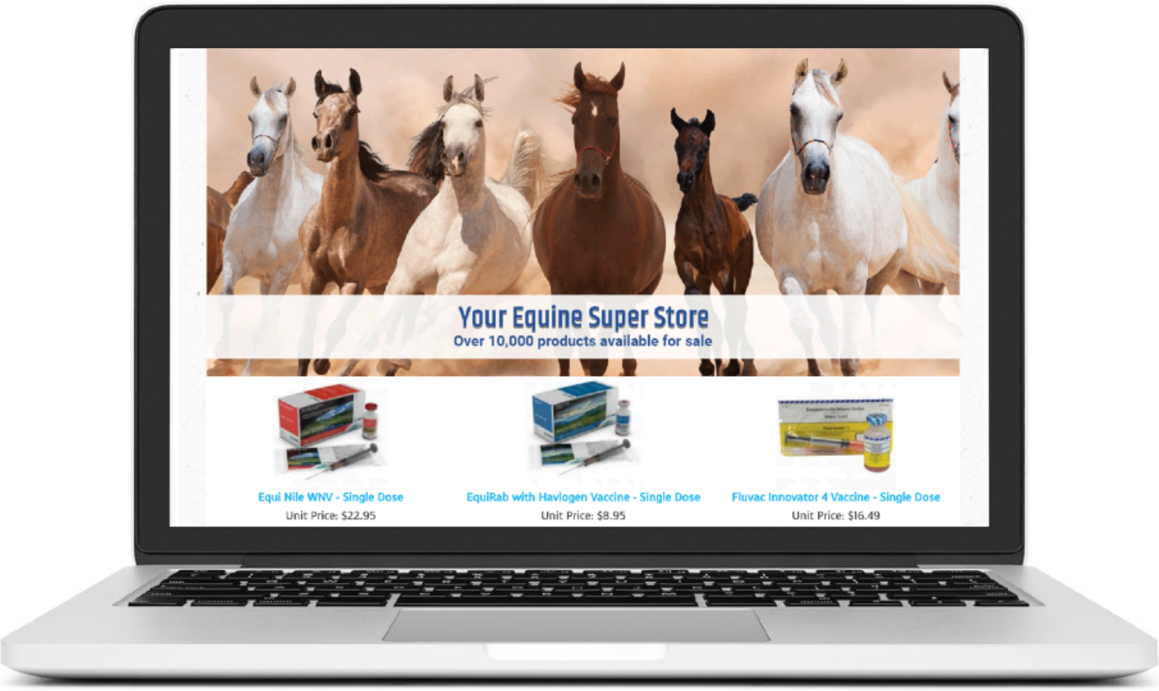
Notably, both accounts LegitScript discovered employed different merchant email addresses. A query for one of those email addresses yielded results showing associations with **other illicit businesses.**

LegitScript's expert analysts knew they were dealing with a zombie transaction launderer, and implemented measures to immediately catch this merchant as soon the merchant attempted to return.

Among these measures, LegitScript:

- Constructed **parsing solutions** that identified new merchants with identical or similar record data;
- Conducted **open-source research** on the entities involved and their known businesses; and
- Collected **DNS information** to proactively identify websites that were under common control but not yet in LegitScript's monitoring portfolio.

Within a week, a new merchant application arrived for a website ostensibly offering **gift cards for sale**; it matched one of the aforementioned criteria. Using information from this new application, LegitScript adapted our existing measures to re-examine our portfolio for other possible matches. We found another merchant seeking to conceal illicit operations by mimicking an existing website selling **equine pharmaceuticals**.


Your Equine Super Store
Over 10,000 products available for sale
Equi Nile WNV - Single Dose
Unit Price: $22.95
EquiRab with Havlogen Vaccine - Single Dose
Unit Price: $8.95
Fluvac Innovator 4 Vaccine - Single Dose
Unit Price: $16.49

Interestingly, this domain name appeared to launder for a **different group** than the gift card TL website, although both were operated by the same principal. This is consistent with LegitScript's findings that individuals often **provide laundering services to multiple illicit networks**. The converse appears to also hold true: illicit networks often **launder through multiple individuals**. For instance, the aforementioned peptides group also engaged in zombie transaction laundering through a consulting website with no discernible ties to any of the other laundering merchants LegitScript identified in this cluster.

Zombie transaction launderers are formidable foes, but ongoing vigilance can thwart illicit activity, break up transaction laundering clusters, and discourage rogue merchants from using your services to conduct cybercrime.

# About LegitScript

At LegitScript, our mission is to make the internet and payment ecosystems safer and more transparent for businesses and internet users.

Our analysts are experts at identifying transaction laundering, and then following threads of data to identify clusters of violative merchants and discourage them from reoffending in your portfolio. We not only proactively monitor for surface-level transaction laundering methods, but also use our expertise to dive deep into complex laundering networks and schemes.

**Contact us** to explore our merchant monitoring service offerings.

## Keep Up-To-Date

**Newsletter: Subscribe**

**Blog: legitscript.com/blog**

**Twitter: @legitscript**

## Contact LegitScript

**Web: legitscript.com/contact**

**Phone: 1-877-534-4879**