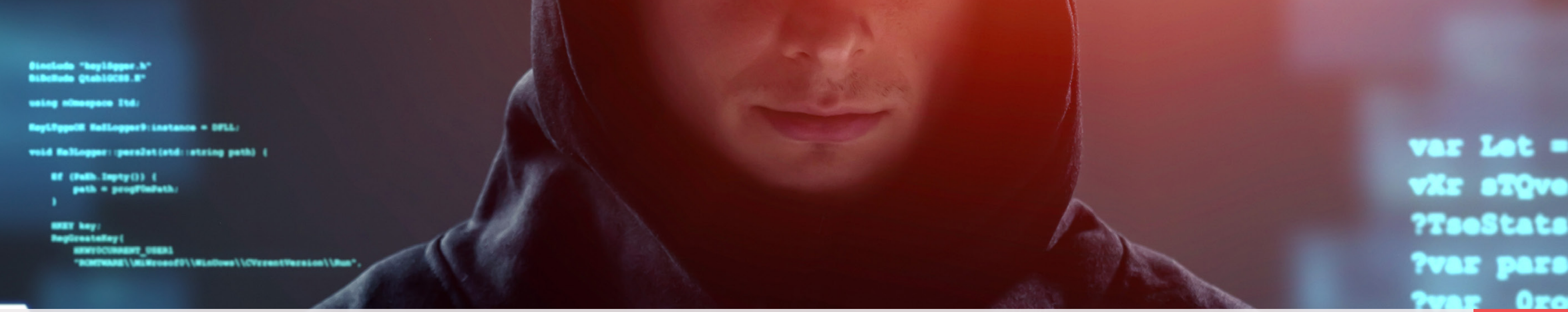


Transaction Laundering: Typologies and Methodologies

Guide

LegitScript

Transaction laundering offers a backdoor into the regulated financial system for cybercriminals who want to offer credit card payments to their customers.

Even as payment processors implement best practices to identify and stop transaction laundering, illicit merchants find new ways to operate and adapt over time. In this guide, we look at common typologies and associated risk factors, evolving transaction laundering methodologies, and key principles you can implement to interrupt and prevent transaction laundering and its associated crimes.

Transaction Laundering: Typologies and Methodologies

Guide

1 Why Transaction Laundering?

More than ever, people are buying online. In 2020, e-commerce accounted for about 20% of retail sales in the United States — totalling about $800 billion — and its share is expected to grow. The internet makes it easy to perpetuate financial crime because it affords anonymity, access to services on the operator’s end, and a much larger pool of customers.

At LegitScript, we often say that illicit sellers are **rational economic actors**. What we mean is that merchants engaged in illicit activity, just like legitimate merchants, are striving to succeed in business. They are making the best possible decisions to ensure their businesses thrive — including a well-built e-commerce website with an easy payment flow. For that reason, problematic merchants want to accept credit card payments.

There are many ways to process payments online, but credit cards are, in most cases, the **gold standard**. Lacking credit card processing, illicit merchants are forced to offer other payment options that are far less desirable for both them and the average customer.

Alternative forms of payment such as eChecks, ACH, or wire transfer are often quite costly to the seller and can take several days to complete the transaction. More tech-savvy customers may know how to use cryptocurrency or peer-to-peer payment methods, but what they offer in increased anonymity and instant processing, they lack in refund and chargeback protections. And, of course, paying cash for an online purchase is virtually unheard of these days.

Credit card
Convenient; ubiquitous; chargeback protection

Cash
Generally not feasible for online businesses

eCheck/ACH
Inconvenient; requires bank account; transations not instant

Wire transfer
Expensive; inconvenient; transactions not instant

Cryptocurrency
Inconvenient; still difficult for non-tech-savvy users

Peer to peer
Inconvenient; lack of chargeback protection

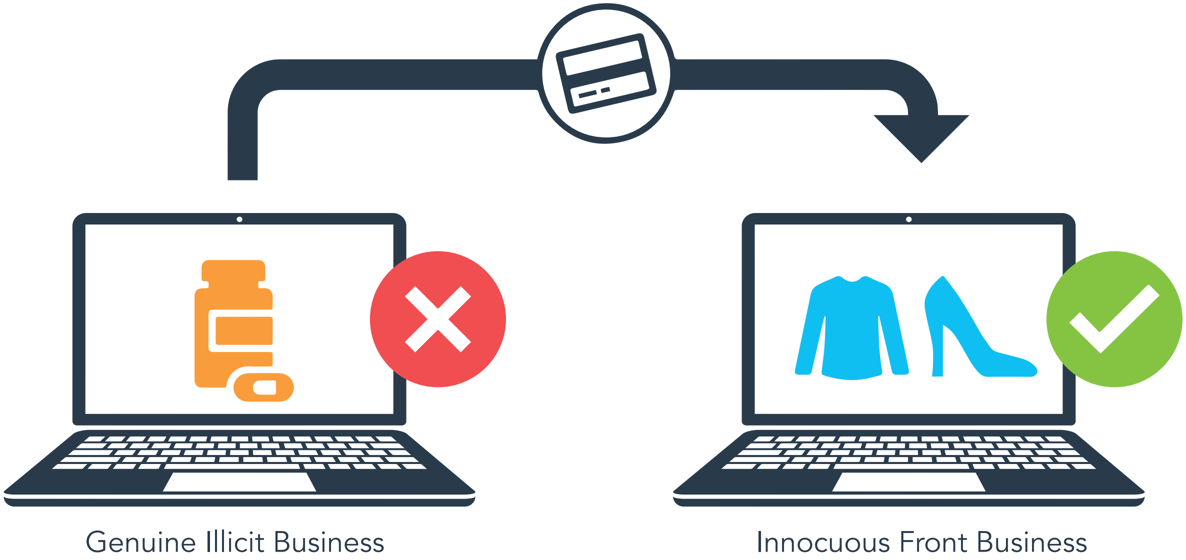
2

Defining Transaction Laundering

At a high level, transaction laundering is a way to **game the payments compliance system**. The illicit merchant obtains a merchant account for a seemingly innocuous business, then uses it to process risky transactions for the true underlying operation.

In many ways, this is analogous to more traditional forms of money laundering, where a front company posing as a genuine business isn't really selling anything, and the payments it takes are actually for something else. A transaction laundering website, commonly referred to as a **bank page**, is the online equivalent of a storefront that — despite never being open, offering strange products that nobody would ever buy, and appearing to have no customers — somehow manages to stay in business.

The increased volume and speed of e-commerce has given rise to **frictionless onboarding**, which enables people to obtain merchant accounts quicker, with less information about them and their business required up front to get started. This is good news for people who are looking for a quick and painless way to get set up with selling online, but it can increase the risk of abuse. Transaction laundering can be challenging to detect even with a more thorough underwriting process, but expedited and frictionless onboarding makes it much easier for illicit actors to exploit the payments ecosystem.



3

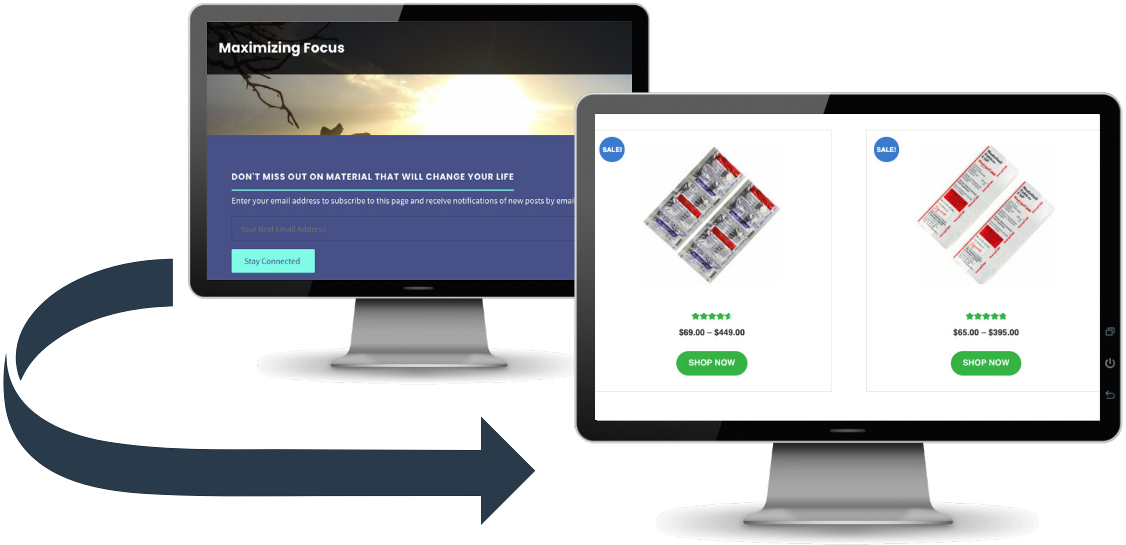
Transaction Laundering Methodologies

Not all transaction laundering looks the same. There are many ways to launder a transaction, and cybercriminals have become increasingly sophisticated in their methods. Let's look at some of the most common ways illicit merchant launder transactions.

Common Methods for Transaction Laundering

1. **The Standard Transaction Laundering Account**

More entrepreneurial illicit merchants may decide to take transaction laundering in their own hands by setting up "bank pages" marketing innocuous goods, but the merchant account information is their real name or business information. This is the type of transaction laundering most of us think about.



Maximizing Focus

DON'T MISS OUT ON MATERIAL THAT WILL CHANGE YOUR LIFE

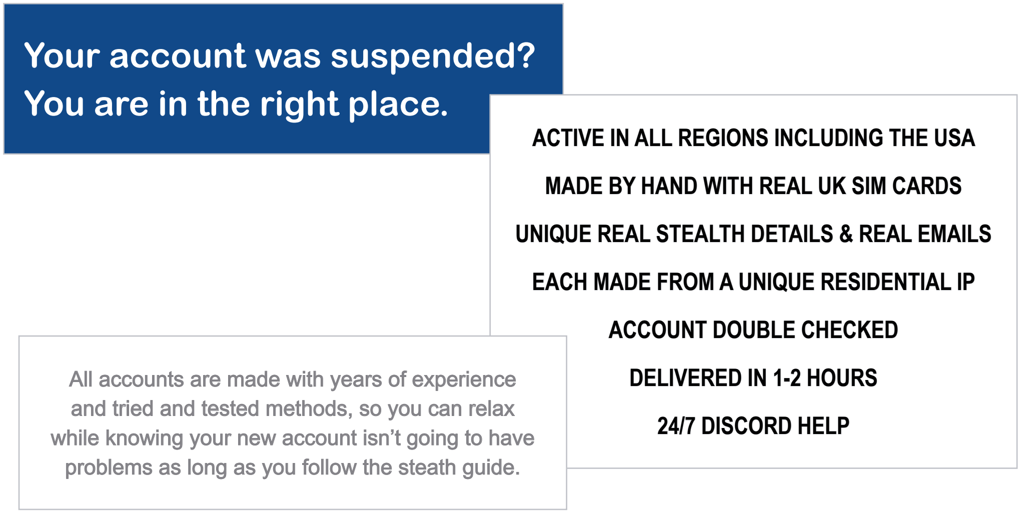
Enter your email address to subscribe to this page and receive notifications of new posts by emai

Case Study: A Modafinil Dealer

The merchant for Maximizing Focus not only used his name in establishing several accounts (that were successively shut down), but eventually recruited his friends' identities once it became evident that he could no longer make accounts under his own name. The problem with this tactic is that he and his friends all live in a small town, which made it easy for LegitScript analysts to spot them as new accounts were created. Furthermore, he would regularly create transaction laundering websites on the same IP address.

2. **The “Stealth” Transaction Laundering Account**

Increasingly, cybercriminals are offering transaction laundering as a service, where an illicit merchant pays to use the payment processing capabilities of a transaction launderer. These types of transaction laundering accounts are sometimes referred to as “**stealth accounts**,” as it’s an easy way to launder under the radar. These transaction launderers typically employ **synthetic identity fraud** — that is, accounts are created with stolen information. It’s “synthetic” because the personal identifiable information (PII) is a mix of random but often authentic information such as birthdays, social security numbers, employer identification numbers, and more. Although real, the information doesn’t necessarily align with any one real person, and it likely comes from data dumps from a variety of breaches. People make these synthetic accounts in bulk and sell them on forums and purpose-built platforms.



Your account was suspended? You are in the right place.

ACTIVE IN ALL REGIONS INCLUDING THE USA

MADE BY HAND WITH REAL UK SIM CARDS

UNIQUE REAL STEALTH DETAILS & REAL EMAILS

EACH MADE FROM A UNIQUE RESIDENTIAL IP

ACCOUNT DOUBLE CHECKED

DELIVERED IN 1-2 HOURS

24/7 DISCORD HELP

All accounts are made with years of experience and tried and tested methods, so you can relax while knowing your new account isn't going to have problems as long as you follow the steath guide.

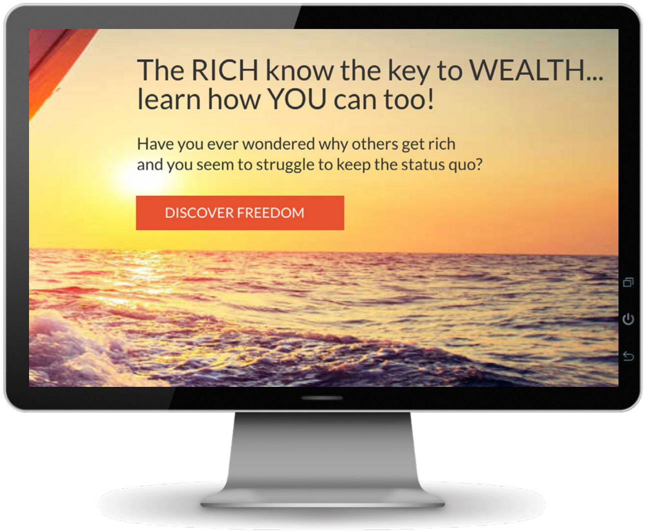
Above is a sampling of copy from websites offering transaction laundering as a service.

Helpful Resources

Synthetic identity fraud is increasingly used to access financial services such as credit, loans, and merchant accounts. Want to learn more about how it is affecting payment processors? Download our guide at legitscript.com/synthetic-id-fraud.

3. **Semi-willing Identity Theft**

LegitScript has seen many instances in which members of the public are recruited online as part of **Independent Business Owner (IBO) schemes**. People lend their identities in the creation of LLCs, which bad actors then use to obtain accounts for processing. IBOs are marketed as "passive income" in the form of commissions on sales from these merchants, but unwitting members of the public typically do not have visibility or understanding into what the accounts are actually being used for. We see IBOs targeting vulnerable populations of US citizens such as the elderly and other fixed- or low-income individuals. See the case study on the following page.



The RICH know the key to WEALTH...
learn how YOU can too!

Have you ever wondered why others get rich
and you seem to struggle to keep the status quo?

Case Study: Financial Freedom or Financial Fraud?

A website offering investment opportunities markets an “IBO 4 Hire” program, promising people the opportunity to make passive income by leveraging their good credit on behalf of companies looking to expand their merchant services. An accompanying video promises monthly income with no effort, but doesn’t explain how the program works, who the partner businesses are, or how a person’s credit will be used. The promise of easy money and an unclear business model puts this opportunity at a high risk of being a transaction laundering service.

4. **Potentially Complicit Payment Processor**

In this scenario, a payment processor may knowingly process payments on behalf of fraud merchants. The processor may not necessarily know the exact nature of the problematic activity but is either permissive or willing to overlook suspicious activity. This type of transaction laundering is rare.

Case Study: Complete Merchant Solutions, LLC

In December 2020, payment processor Complete Merchant Solutions (CMS) and its CEO agreed to pay $1.5 million to the Federal Trade Commission to settle charges the company facilitated fraud. The FTC charged that CMS "illegally processed millions of dollars in consumer credit card payments for fraudulent schemes when they knew or should have known that the schemes were defrauding consumers." Furthermore, the FTC stated that CMS "ignored clear red flags of illegal conduct by those schemes, such as high rates of consumer chargebacks, use of multiple merchant accounts to artificially reduce chargeback rates so as to evade detection by banks and the credit card associations, submission of sham chargeback reduction plans, and the use of merchant accounts to process payments for products and services for which the merchant did not get approval from the bank holding the accounts."

How Merchants Adapt When Detected

Regardless of the method, illicit merchants processing payments using transaction laundering are resilient and typically have techniques to adapt when caught. The most common responses include:

1. Creating **more transaction laundering websites**. Recent domain name creation dates may be a clue for merchants who are operating on the fly.

2. Setting up an arsenal of **transaction laundering accounts** for load balancing, and to protect against the possibility of accounts being closed.

3. Taking **other payment methods** such as peer-to-peer and cryptocurrencies as a stopgap until the merchant regains credit-card processing.

4

Transaction Laundering Typologies

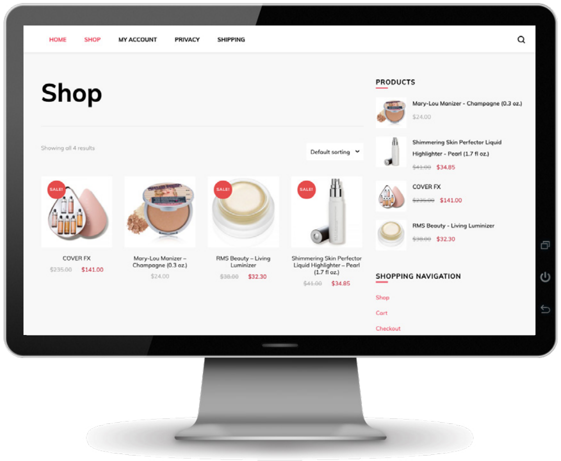
Transaction laundering is a technique employed by a variety of cybercriminals, from merchants selling illicit drugs to ones offering illegal gambling. It's helpful to understand that each type of illicit merchant tends to act in a **particular way** and employ **common techniques** that may help you to more quickly identify them. For example, cybercriminals selling IP-infringing streaming entertainment often set up merchant websites for vague computer services, such as web hosting or technical support.

Let's look at some of the most common typologies of transaction launderers and how each type tends to operate.

Rogue Internet Pharmacies

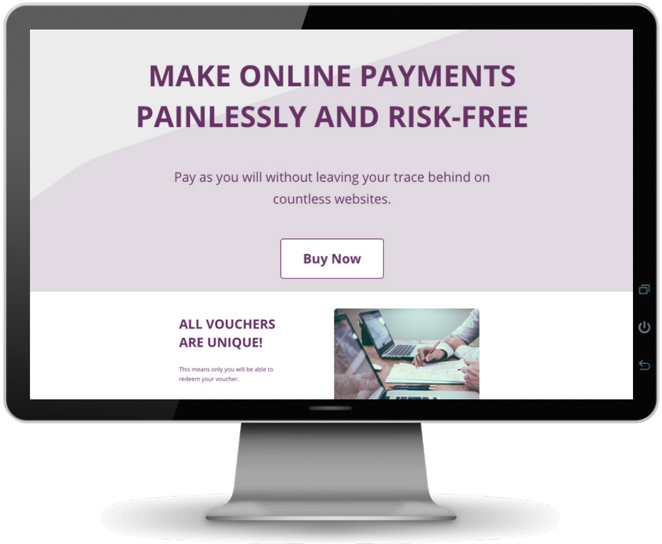
Rogue internet pharmacies are ones that offer pharmaceuticals illegally — that is, selling without a valid prescription requirement, selling in a jurisdiction where they are unlicensed, and/or selling unapproved drugs. The screenshot shown here is of a cosmetics website that was transaction laundering for a merchant offering controlled substances and opioids via email solicitations. See our case study on page 27 for more on this merchant.

- Common typology: health- and wellness-related websites selling supplements or cosmetics, enabling the merchant to have a plausibly related merchant descriptor
- Whois/DNS research may reveal affiliated websites



Illicit Gambling

A common type of laundering seen with gambling merchants is the use of intermediary payment forms, or payment aggregation methods, to obscure illicit transactions. Merchants are blocked from accepting credit cards for gambling in some jurisdictions, so they will direct users to pay for an e-voucher, or will route them through a cryptocurrency exchange that takes payments via credit card. As shown in the screenshot, risky stored value or aggregation services are often used.



MAKE ONLINE PAYMENTS PAINLESSLY AND RISK-FREE

Pay as you will without leaving your trace behind on countless websites.

ALL VOUCHERS ARE UNIQUE!

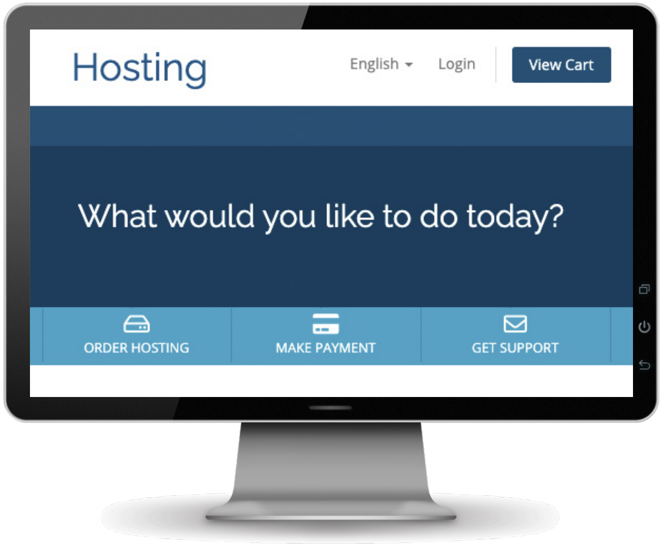
This means only you will be able to redeem your voucher.

It's not unusual for us to see a **highly integrated payment processing flow**. For example, upon attempting a deposit on a gambling website with a card, we are redirected to a crypto exchange for the same amount, and then routed back to the gambling website when the exchange is complete. Although it's possible that some of these exchanges are genuine cryptocurrency marketplaces, most that we encounter with gambling website integration appear purpose-driven for laundering.

- Common typology: risky stored value products such as e-vouchers or aggregation services
- Laundering can occur through credit cards used on a cryptocurrency wallet integrated with a gambling website
- Online gambling is also used for money laundering

IP-infringing IPTV

Illicit IPTV is persistently one of the **most common services** to make use of transaction laundering. According to the International Trademark Association, the total estimated value of counterfeit and pirated goods, including digital piracy, is nearing $3 trillion, with illicit streaming entertainment responsible for an increasing share. Merchants offering IP-infringing IPTV often use web hosting or VPS services as a laundering guise for IPTV resellers, as shown in the screenshot.



What would you like to do today?

Rights holders are also fighting back against piracy, and payment processors may be left on the hook for sizable fines associated with helping to facilitate these sales. Both Visa and Mastercard prohibit illegal transactions involving copyright infringement, and work diligently with rights holders to investigate allegations of infringing behavior. Regulatory agencies may also hold internet companies accountable if they show gross negligence in allowing these merchants to market or conduct business on their platforms.

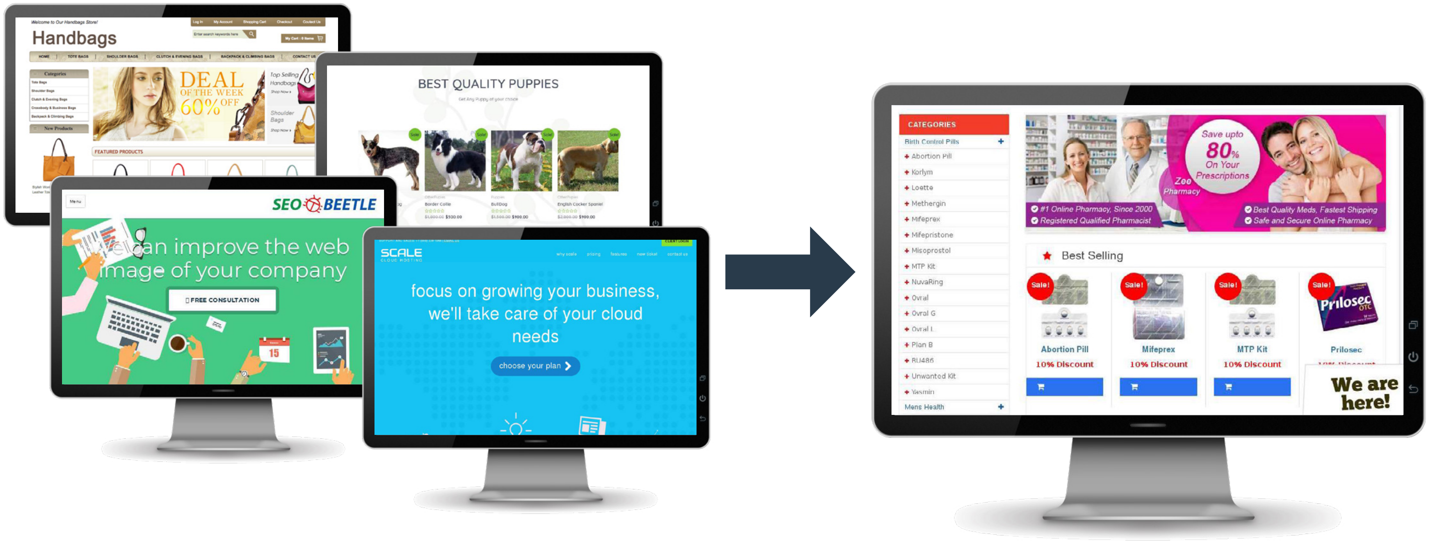
- Common typology: subscription-based fronts such as web hosting for IPTV processing
- Web hosting is particularly common
- Automatic redirects may occur at checkout

Negative-option Billing

A potentially deceptive approach to selling, negative-option billing can ensnare consumers in ongoing subscriptions without their express consent. The Federal Trade Commission has highlighted the practice as a major focus of enforcement, and Mastercard made changes to its standards regarding the registration of negative-option merchants. These merchants operate a bit differently in that they often create multiple **innocuous-seeming storefronts** so that they can engage in load balancing. The screenshots on the following page show websites offering everything from handbags to pets, but all of them were processing payments for a website marketing high-risk sexual health products.

Helpful Resources

Want to learn more about negative-option billing? Download our guide, which details card brand rules and regulatory actions, at legitscript.com/negative-option-billing.



- Common typology: A variety of websites that look innocuous but with offerings that may seem strange under closer scrutiny

- Merchants engaged in deceptive recurring billing schemes also pose a high risk for chargebacks.

- To prevent detection, merchants will create many storefronts to rotate their payments through to engage in load balancing.

5 Red Flags of Transaction Laundering

Although transaction launderers are pernicious because of their ability to evade detection, certain types of business models **inherently pose elevated risk** for transaction laundering because they are so easy to abuse. They include:

- Drop-shipping
  - Especially consumer goods such as clothing, electronics, and knickknacks
- Generic technical services such as web design, hosting, or SEO
- Generic professional services such as graphic design
- Lower-risk healthcare products such as supplements and cosmetics

For these types of businesses, a **face-value analysis** can offer important clues about whether a website warrants additional scrutiny. There are ways to differentiate incomplete websites from potential bank pages. Some of these include:

- Use of a generic template-based website with little modification
- Website copy and design that is not consumer-friendly, lacking expected dynamic features
- Lack of a greater web presence, such as social media profiles and consumer reviews
- Website configurations that prevent web crawlers from indexing the page

If a face-value analysis raises red flags, a **network-mapping analysis** can help reveal if the website is connected to anything else of note. This can be done with open-source information alone — such as searching for contact information published on the website that shows up elsewhere.

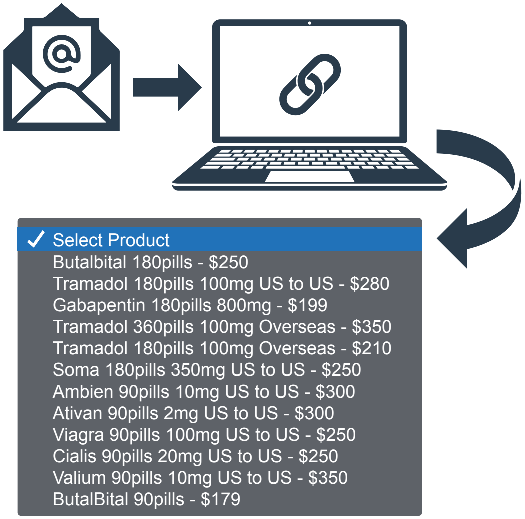
Other points of inquiry can include **website infrastructure** and **technical data analysis**, as it's not uncommon for merchants to reuse the same services for their transaction laundering websites as well as those offering violative products. Merchant application details can also prove valuable since many merchants are unaware that investigators may have visibility into this data, and so they may leave obvious clues. So, remember to research:

- Published contact information on the merchant's website
- Merchant application details
- Technical data such as Whois, web hosting, and DNS for connections to other websites
  - This might reveal connections directly to the underlying violative website, or, alternatively, to a ring of transaction laundering websites.

Case Study: Drugs Via Email

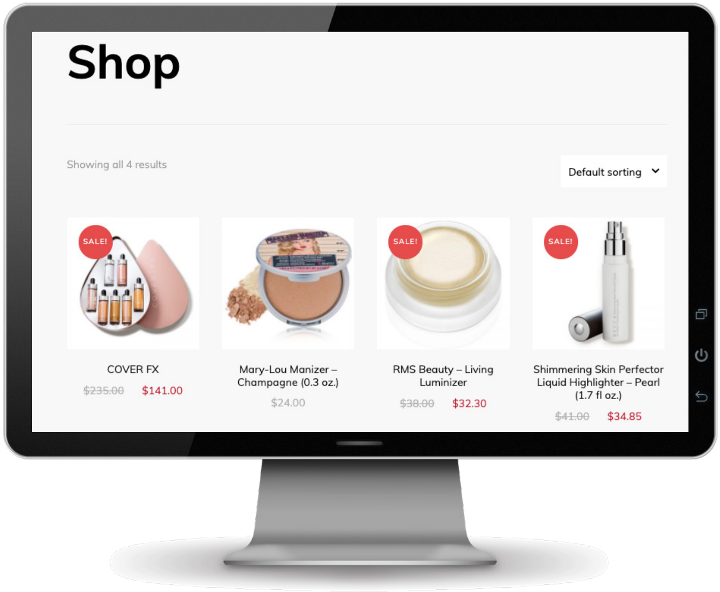
Large transaction laundering schemes can be uncovered through a single bad actor. This case study provides an example of how a transaction laundering investigation can begin with a single website or merchant account, and grow to include a full network of illicit activity.

LegitScript received an email solicitation to an undercover account from a merchant offering prescription opioids, such as tramadol, for sale to consumers in the US. The rogue pharmacy operation provided a URL in the body of the email that was inaccessible through the root domain, but allowed customers with a link to a specific web page to place orders.



✓ Select Product
Butalbital 180pills - $250
Tramadol 180pills 100mg US to US - $280
Gabapentin 180pills 800mg - $199
Tramadol 360pills 100mg Overseas - $350
Tramadol 180pills 100mg Overseas - $210
Soma 180pills 350mg US to US - $250
Ambien 90pills 10mg US to US - $300
Ativan 90pills 2mg US to US - $300
Viagra 90pills 100mg US to US - $250
Cialis 90pills 20mg US to US - $250
Valium 90pills 10mg US to US - $350
ButalBital 90pills - $179

A test transaction returned a merchant descriptor corresponding to a generic cosmetics website. This website bore hallmarks of transaction laundering, such as a bare-bones product listing and incongruous product pricing. That is to say, the face-value analysis raised red flags.



Shop

Showing all 4 results

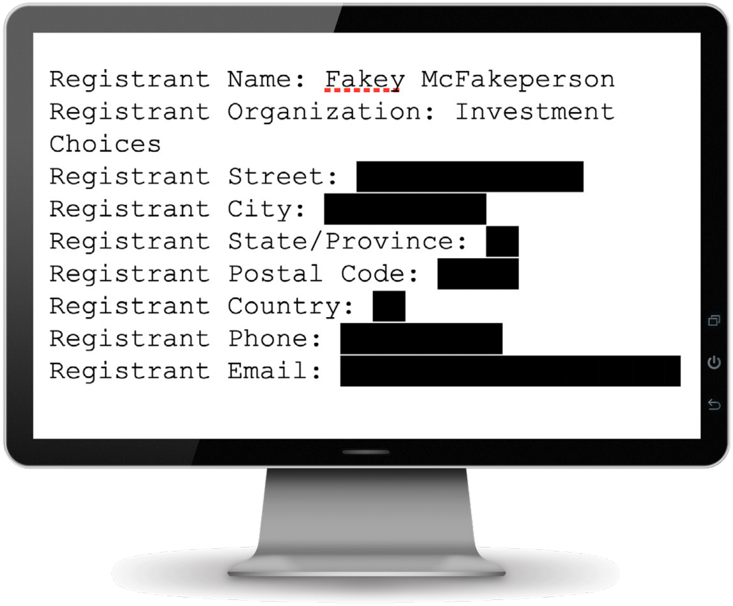
COVER FX
~~$235.00~~ $141.00

Mary-Lou Manizer – Champagne (0.3 oz.)
$24.00

RMS Beauty – Living Luminizer
~~$38.00~~ $32.30

Shimmering Skin Perfector Liquid Highlighter – Pearl (1.7 fl oz.)
~~$41.00~~ $34.85

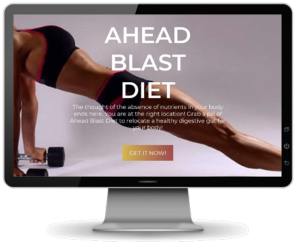
Next, we performed a network-mapping analysis. Details and published contact information on the website were generally unattributable. Whois registration information* provided an additional avenue for investigation. More than 20 additional domain names pointing to websites with hallmarks of transaction laundering are, or were historically, registered using these contacts.



```
Registrant Name: Fakey McFakeperson
Registrant Organization: Investment
Choices
Registrant Street: [redacted]
Registrant City: [redacted]
Registrant State/Province: [redacted]
Registrant Postal Code: [redacted]
Registrant Country: [redacted]
Registrant Phone: [redacted]
Registrant Email: [redacted]
```

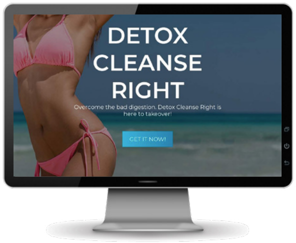
*Names altered because of sensitive information.

Several websites stood out as outliers, including one offering high-risk merchant processing, and another offering an "investment opportunity" wherein individuals could provide their identity and credit to "partner in" a merchant account for unknown businesses. (This was the IBO scam mentioned earlier in this guide.)



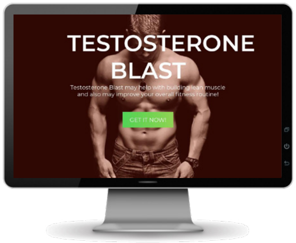
AHEAD BLAST DIET

The thought of the absence of nutrients in your body ends here. You are at the right location! Grab a pill of Ahead Blast Diet to relocate a healthy digestive gut for your body!



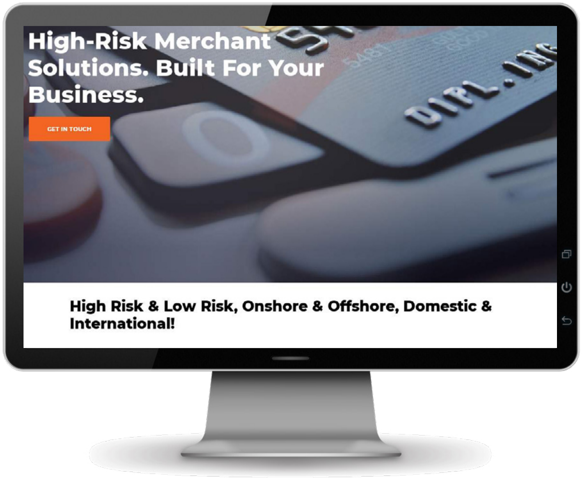
DETOX CLEANSE RIGHT

Overcome the bad digestion. Detox Cleanse Right is here to takeover!



TESTOSTERONE BLAST

Testosterone Blast may help with building lean muscle and also may improve your overall fitness routine!



High-Risk Merchant Solutions. Built For Your Business.

High Risk & Low Risk, Onshore & Offshore, Domestic & International!

One domain name actually bore the business name listed in the Whois; the other website offered access to high-risk merchant accounts — suggesting that this was an integrated operation that sought IBOs for merchant accounts, set up fake bank pages, and then offered the accounts to merchants looking to process cards for all manner of things (including, to our knowledge, illicit pharmaceutical sales).

While websites in this network have been taken down, the operation is still live as of the publishing of this guide. LegitScript continues to track this network of transaction laundering websites and illicit businesses to help our clients steer clear of this activity.

About LegitScript

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

LegitScript has created the world’s leading team of experts to detect merchants engaged in transaction laundering and other forms of cybercrime. That’s why LegitScript is used, trusted, or recommended by major card brands to help payment service providers monitor for high-risk merchants to determine which are in compliance and which aren’t.

Contact Us

Phone: 1-877-534-4879
Web: **legitscript.com/contact**

Keep Up to Date

Newsletter: **legitscript.com/newsletter**
Blog: **legitscript.com/blog**
Twitter: **@legitscript**

You may also be interested in:

How LegitScript Uncovered a Massive Transaction Laundering Network

How LegitScript Uncovered a Massive Transaction Laundering Network

Case Study

LegitScript

Contact us to get your copy.