Five Ways Cybercriminals Trick Monitoring Algorithms

David Khalaf, LegitScript

LegitScript

Today’s Presenter

David Khalaf

Communications and
PR Manager

EXPERT INSIGHT

We combine big data, advanced technology, and expert human analysis so you can confidently assess merchant risk and take action before it results in fines.

Algorithm-only solutions simply can't keep up.

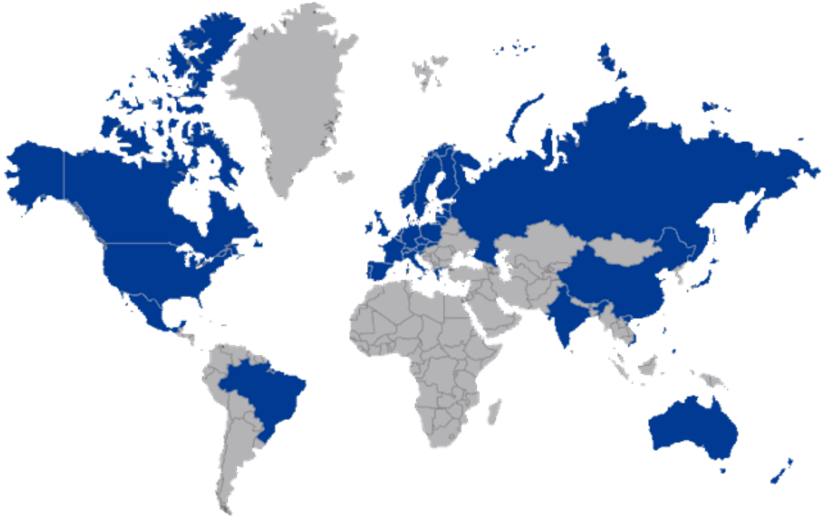
Monitoring Coverage

EXPERTISE IN 60+ HIGH RISK AREAS

Including but not limited to:

- Adult and Illegal Adult
- Aggregation
- Alcohol
- Bail Bonds
- CBD
- Collection Services
- Computer Technical Support
- Controlled Substances
- Coronavirus/COVID-19
- Cosmetics
- Credit Services
- Cyberlockers
- Drop-shipping/Freight-forwarding
- Drug Paraphernalia
- Embassy Services
- Escorts
- Essay Mills
- Eyeglasses/Contact Lenses
- Fireworks
- Fraud
- Gambling
- Get-Rich-Quick Schemes
- Hate/Harm
- Hazardous Materials
- Healthcare Products
- Intellectual Property
- Investment Opportunities
- Lead Generation
- Lending
- Live Animals
- Marijuana
- Medical Services
- Multi-level Marketing
- Money Services
- Mugshot Publication
- Negative Option
- No Value Added
- Psychic/Occult
- Psychoactive Highs
- Smokes
- Social Media Buys
- Stored Value
- Travel
- Virtual Credits/Cryptocurrency
- Weapons

COVERAGE IN 100+ COUNTRIES



AND 15+ LANGUAGES

HOW CYBERCRIMINALS TRICK ALGORITHMS

TRICK #1

CREATING MULTIPLE MERCHANT ACCOUNTS

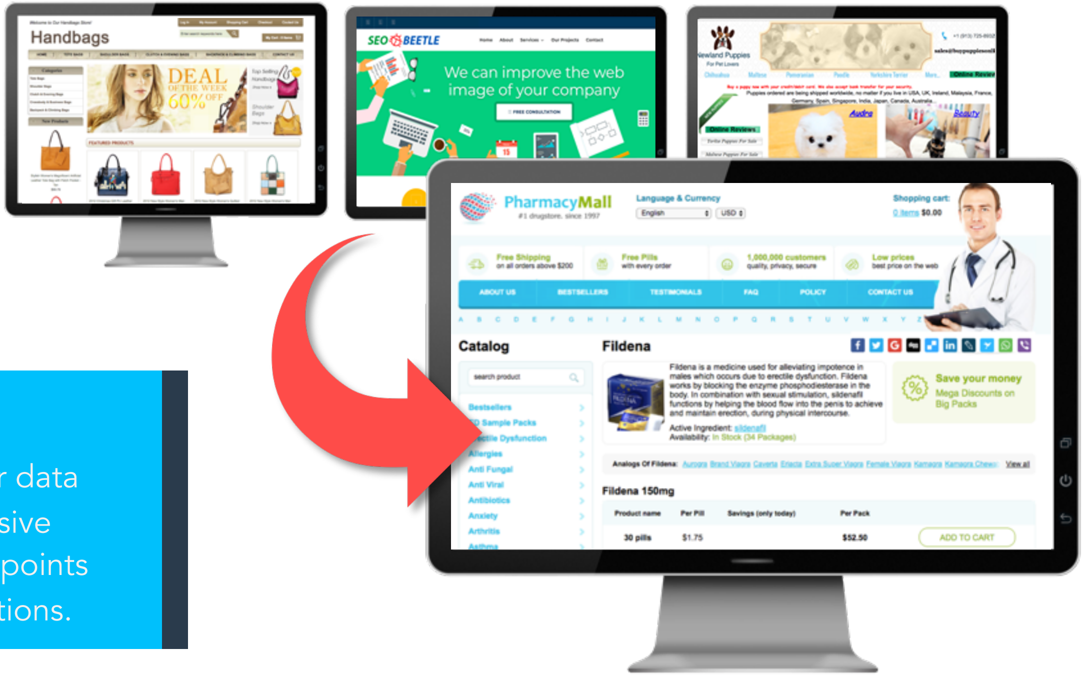
Some cybercriminals create many genuine-seeming business accounts and then get multiple merchant accounts to load-balance high-risk transactions.

Load Balancing With Multiple Accouts

- The merchant launders money among multiple accounts.
- Alternatively, a merchant may use falsified but real business information.
- It's difficult for an algorithm to flag seemingly legitimate business info.

HOW TO STOP IT

LegitScript's expert analysts can spot irregular data points in business information, and our extensive network-mapping intel helps us identify data points that connect merchants to known illicit operations.



TRICK #2

DISTANCING THE CRIME FROM THE PAYMENT

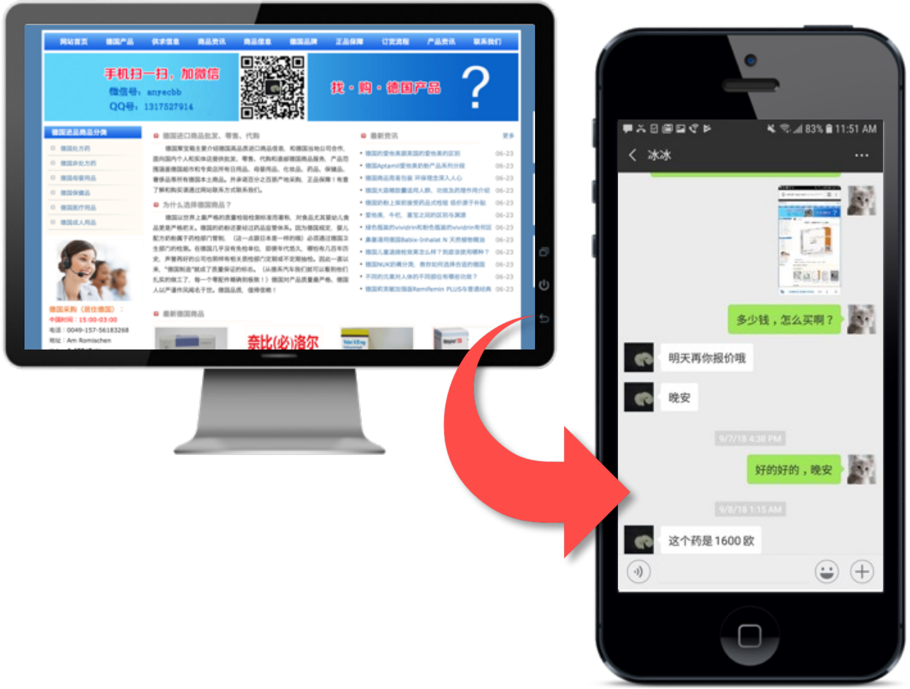
Some merchants have innocuous-looking websites that drive customers to other technology to complete a transaction (e.g., What's App, phone call, etc.).

Distancing Violative Products or Services

- Innocuous websites can drive customers to other communication platforms to market illicit products or services and process the transaction.
- A merchant may also use problematic marketing online to drive traffic to an innocuous-seeming website.

HOW TO STOP IT

LegitScript monitors not only payment ecosystems, but advertising and other data points across the internet so that we have a more holistic view of a merchant's operations.



多少钱，怎么买啊？

明天再你报价哦

晚安

9/7/18 4:38 PM

好的好的，晚安

9/8/18 1:15 AM

这个药是 1600 欧

TRICK #3

OVERT METADATA IN SOURCE CODE

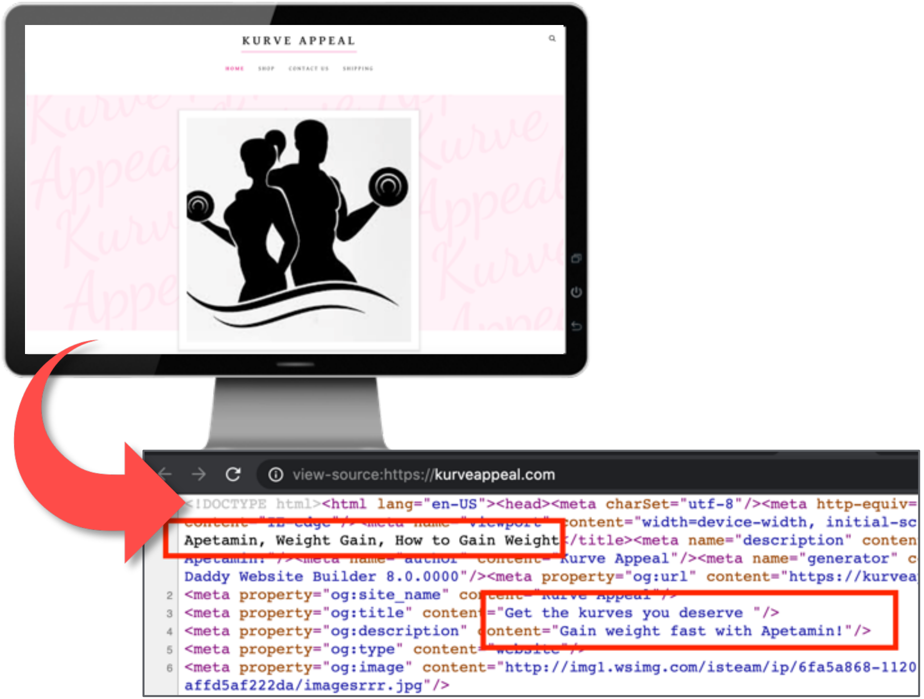
A merchant may use innocuous or coded language on the visible website, but use overt keywords in the metadata to help with search engine optimization.

Using Metadata to Hide a Website’s Intent

- Metadata is a set of data that describes and gives information about other data.
- Search engines read metadata, making it important for search engine optimization (SEO).
- Algorithms won’t always catch metadata, or if they do it’s up to the payments risk team to figure why a website was flagged.

HOW TO STOP IT

LegitScript’s human analysts can recognize coded language such as “targeted weight gain” and know to search the metadata for evidence of a website’s intended purpose.



```
<!DOCTYPE html><html lang="en-US"><head><meta charSet="utf-8"/><meta http-equiv=
content="IE=edge"/><meta name="viewport" content="width=device-width, initial-sc
Apetamin, Weight Gain, How to Gain Weight</title><meta name="description" conten
Apetamin!"/><meta name="author" content="Kurve Appeal"/><meta name="generator" c
Daddy Website Builder 8.0.0000"/><meta property="og:url" content="https://kurvea
<meta property="og:site_name" content="Kurve Appeal"/>
<meta property="og:title" content="Get the kurves you deserve "/>
<meta property="og:description" content="Gain weight fast with Apetamin!"/>
<meta property="og:type" content="website"/>
<meta property="og:image" content="http://img1.wsimg.com/isteam/ip/6fa5a868-1120
affd5af222da/imagesrrr.jpg"/>
```

TRICK #4

USING SOCIAL MEDIA FOR ILLICIT ACTIVITY

A website may have an innocuous catalog, but the merchant may be marketing illicit products or services on their social media profiles.

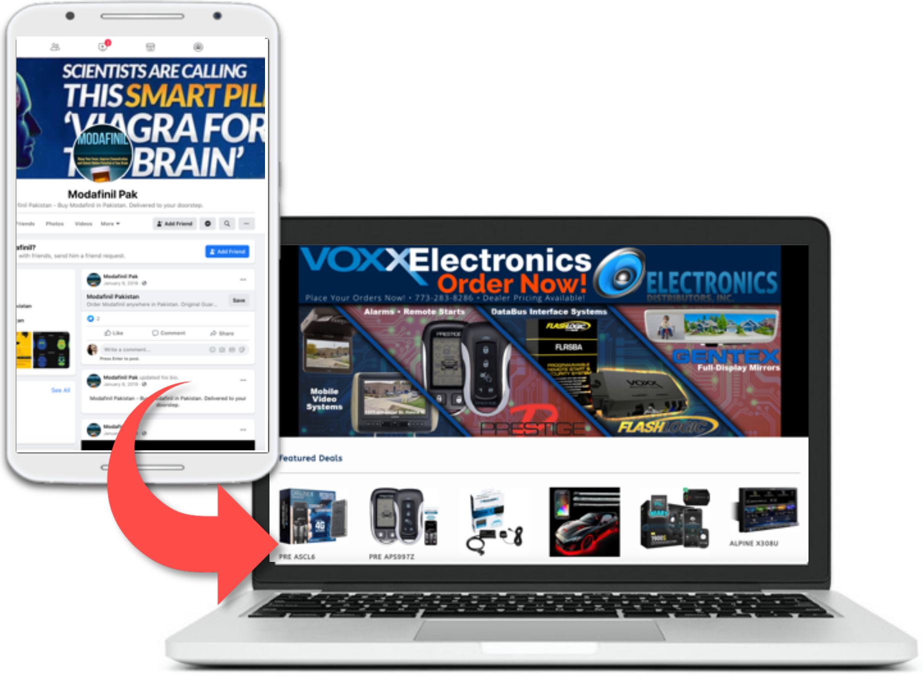
LegitScript

Using Social Media for Illicit Activity

- A merchant can use social media to market illicit products or services. For example, a merchant marketing modafinil on social media could instruct customers to purchase a particular product from their electronics website receive the illicit product.
- Only investigation beyond a merchant's website can reveal this kind of illicit activity.

HOW TO STOP IT

LegitScript's expert analysts conduct open-source research to detect this kind of activity, and LegitScript's monitoring of major internet platforms helps to identify this activity for clients early on.


SCIENTISTS ARE CALLING THIS SMART PIL 'VIAGRA FOR T BRAIN'
MODAFINIL
Modafinil Pak
Modafinil Pakistan - Buy Modafinil in Pakistan. Delivered to your doorstep.
Add Friend
Modafinil Pak
Modafinil Pakistan
Save
Like
Comment
Share
Write a comment...
See All
VOXXElectronics
Order Now!
ELECTRONICS DISTRIBUTORS, INC.
Place Your Orders Now! • 773-283-8286 • Dealer Pricing Available!
Alarms • Remote Starts
DataBus Interface Systems
Mobile Video Systems
GENTEX Full-Display Mirrors
PRESTIGE
FLASHLOGIC
Featured Deals
PRE ASCL6
PRE APS997Z
ALPINE X308U

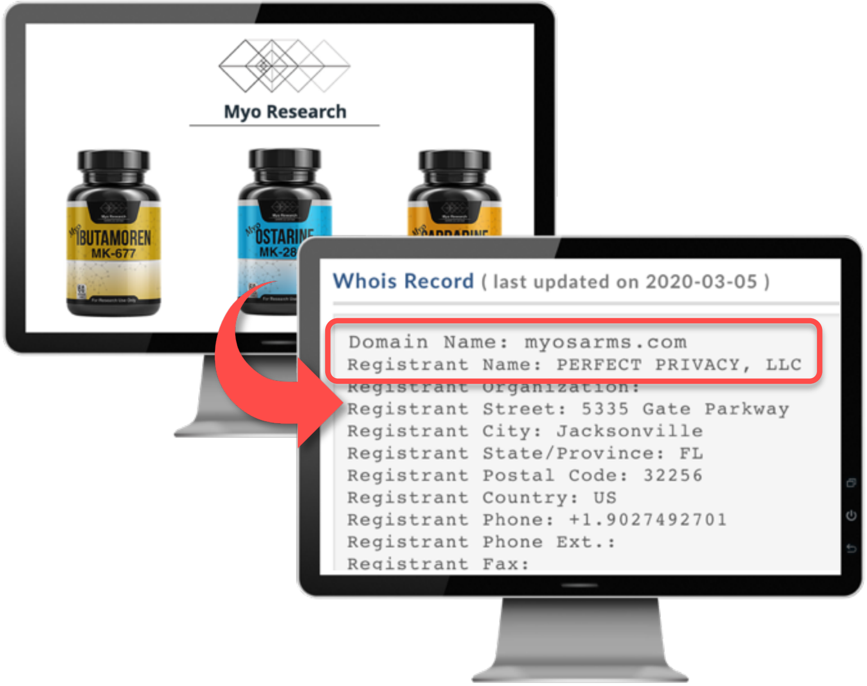
TRICK #5

UNATTRIBUTABLE TECHNICAL CONFIGURATIONS

In the absence of reliable, publicly accessible Whois info and the increasing use of large e-commerce platforms, simple technical risk indicators aren't always enough to make the connection to a bad actor.

Anonymity With Technical Configurations

- Government regulations and privacy servers make it increasing difficult to know who operates a website.
- Large e-commerce platforms often have shared/unattributable internet infrastructure.



Whois Record (last updated on 2020-03-05)

```
Domain Name: myosarms.com
Registrant Name: PERFECT PRIVACY, LLC
Registrant Organization:
Registrant Street: 5335 Gate Parkway
Registrant City: Jacksonville
Registrant State/Province: FL
Registrant Postal Code: 32256
Registrant Country: US
Registrant Phone: +1.9027492701
Registrant Phone Ext.:
Registrant Fax:
```

HOW TO STOP IT

LegitScript has the world's largest database of cybercrime networks. Our historical data allows us to make connections that wouldn't otherwise be possible.

LegitScript

LEARN MORE FROM THE EXPERTS

LegitScript

LegitScript Merchant Website Analysis Tip Sheet

Reviewing merchant websites can be both difficult and time consuming. LegitScript's checklist gives you tools to more easily identify common red flags for merchants engaged in high-risk businesses. Have questions about other high-risk categories? Ask us at legitscript.com/contact.

Tips for Supplement/ Pharmaceutical Websites

- □ **Search the merchant URL at legitscript.com.** Our database can show if the website is a LegitScript-certified pharmacy or a rogue internet pharmacy.
- □ **Search products on legitscript.com.** For supplements, pay particular attention to high-risk products such as pre-workouts, muscle builders, weight-loss products, and sexual health products.
- □ **"Site:" search the website.** Enter "site:[merchant domain name]" in a web browser to see results for subpages of the website. This may reveal hidden and potentially violative pages that are otherwise undiscoverable through normal navigation.
- □ **Search contact information.** Google unique contact information such as email addresses and phone numbers. This may help you identify affiliated websites, social media, customer complaints or other online content to give you a broader picture of the merchant's operation.
- □ **Read the copy.** For supplement websites, read product descriptions for language stating that a product can prevent, cure, treat, or mitigate diseases. These may be problematic claims.

Tips for Deceptive/Scammy Websites

- □ **Search for business registration information.** Websites such as opencorporates.com can show if a business is properly registered and to whom. See if the principals have other business registrations and, if so, research what those businesses are.
- □ **Search the IP address.** Websites such as bgp.he.net can show you a domain name's IP address and list what other domain names are on that IP address or adjacent IP addresses. Scan the list for potentially problematic websites, especially ones offering the same or similar products or services.
- □ **Check consumer complaints.** Websites such as ripoffreport.com and bbb.org record customer complaints against businesses, which may reveal a business' operational methods.
- □ **Search contact information.** Google unique contact information such as email addresses and phone numbers to identify affiliated websites or other relevant online content. If there is no contact information listed on the website or it is difficult to find, that may be a red flag.
- □ **Read the offer.** Examine the language describing the service or product. Does it sound too good to be true? Are the terms and conditions complex and confusing? Does the service or product promise to help customers circumvent known laws or expedite regulatory processes? These may be red flags.

Tips for Innocuous/Other Websites

- □ **Check domain name registration information.** Websites such as whois.com may show to whom a domain name is registered. If the domain name is privacy-protected, or if you want to dig further, research the domain name's IP address (see instructions above).
- □ **"Site:" search the website.** See the instructions in the Supplement/Pharmaceutical section.
- □ **Search contact information.** See the instructions in the Deceptive/Scammy section.
- □ **Review social media.** Most businesses have social media accounts. Review the content on these for problematic offers, products, or other possible affiliated websites. Businesses with no social media or other internet presence may be a red flag.
- □ **Pretend to be a customer.** Go through the website like a customer would to gauge the user experience. Look for red flags such as illogical prices, a limited product lineup, neglected or incomplete pages, and strange or missing payment options.

CHECKLIST FOR RISK TEAMS

Merchant Website Analysis Tip Sheet

Get useful tips in a checklist format to help your risk team more easily identify common red flags for merchants engaged in high-risk businesses.

Download at:
legitscript.com/analyst-checklist

LegitScript