LegitScript

CASE STUDY · PLATFORM RISK SOLUTIONS

Inside the Fake ID Network:

From Isolated Signal to Coordinated Disruption

THE PREMISE

What initially looked like a few isolated accounts promoting fake IDs on one of the world's largest platforms ultimately turned out to be a large coordinated network with presence in China and the US, an affiliated/reseller program on multiple platforms, suspected transaction laundering websites, and more than 90 connected websites. Keep reading to learn what happens when fraud evades controls, and when network intelligence reveals the gaps.

INVESTIGATION LIFECYCLE

SIGNAL

A cluster of social accounts promoting **fake government IDs** including Green Cards, SSNs, driver's licenses. Accounts appeared isolated but shared language patterns, and consistent off-platform redirects raised flags that suggested coordination.

EXPANSION

LegitScript investigators moved off-platform. External URLs referenced in profiles connected to **90+ websites** linked by shared IP infrastructure, reused contact data, and domain redirect chains. Cross-platform reseller accounts **all funneled into the same ecosystem**.

HUMAN VALIDATION

Registered business activity detected as leather wallet manufacturing had **no relationship to the products being sold**. Structured affiliate programs, centralized control, and high website volume confirmed **coordinated operation** rather than coincidence.

INTELLIGENCE DELIVERY

A **structured intelligence report** containing a full network map, technical indicators, and relationship documentationwas delivered to the platform partner, enabling scaled enforcement and detection tuning.

ENFORCEMENT ACTION

Accounts and infrastructure **removed collectively as an interconnected operation**. Network signals incorporated into proactive detection systems, preventing re-entry at scale.

KEY FINDINGS

NETWORK INFRASTRUCTURE

- Shared IP addresses indicating centralized hosting across **90+ domains**
- **Reused contact information** across the full network; phone numbers, email addresses, registrant data
- **Domain redirect chains** connecting surface presence to operational core
- **Operational nodes** confirmed in both US and China

BUSINESS MODEL INDICATORS

- Structured **affiliate and reseller program** operating across multiple platforms
- **Deliberate obfuscation:** registered as consumer goods, operating as a documnet fraud network
- **Off-platform fulfillment** via encrypted messaging apps and redirect sites
- Marketing explicitly **directed at minors** — a deliberate legal exposure

> ***"Every signal had an innocent explanation. It was the pattern across all of them that made the case."***
>
> LEGITSCRIPT INVESTIGATION TEAM

ENFORCEMENT OUTCOMES

ACCOUNTS
Additional accounts identified beyond on-platform monitoring

NETWORK
Full network removed entirely, not as isolated violations

DETECTION
Network signals fed into proactive detection systems

INTELLIGENCE
Each investigation is a durable asset for future enforcement