OneRisk

PRODUCT OVERVIEW

Merchant fraud detection that starts with the entire internet

OneRisk maintains intelligence on every active online merchant, links the storefronts that share supporting infrastructure, and gives acquirers, payment facilitators and ISOs the evidence to identify fraudulent merchants in their portfolios and pipelines.



01 / A NEW APPROACH

Start from the storefront, not the application

Conventional underwriting evaluates what an applicant chooses to disclose: the application, the website it lists and the documentation it supplies. Fraudulent merchants are built to pass those checks. They present a compliant website for underwriting, route sales from undisclosed storefronts through the approved merchant account and reapply under new identities after termination. OneRisk starts from the storefronts themselves, whether they have ever applied for a merchant account.

	CONVENTIONAL SCREENING	ONERISK
Starting point	The merchant's application	Every online merchant on the internet
What it sees	The website the applicant names	Every storefront the operator runs
When it looks	At onboarding and periodic review	At onboarding, then continuously
What it returns	A pass or fail against a checklist	A risk rating with reason codes and evidence

02 / CENSUS

Every online merchant, already on file

Census is OneRisk's continuously refreshed registry of online merchants. It has evaluated more than 269 million domains and identified more than 22 million active online merchants, including storefronts no acquirer has underwritten. An identifier observed on one storefront can be traced to every merchant site that shares it.

03 / MERCHANT PROFILES

Every merchant, assessed and explained

Each merchant is assessed across eight risk dimensions, from website content and hosting to payment configuration and network linkage, and every rating is explained and supported by reason codes.

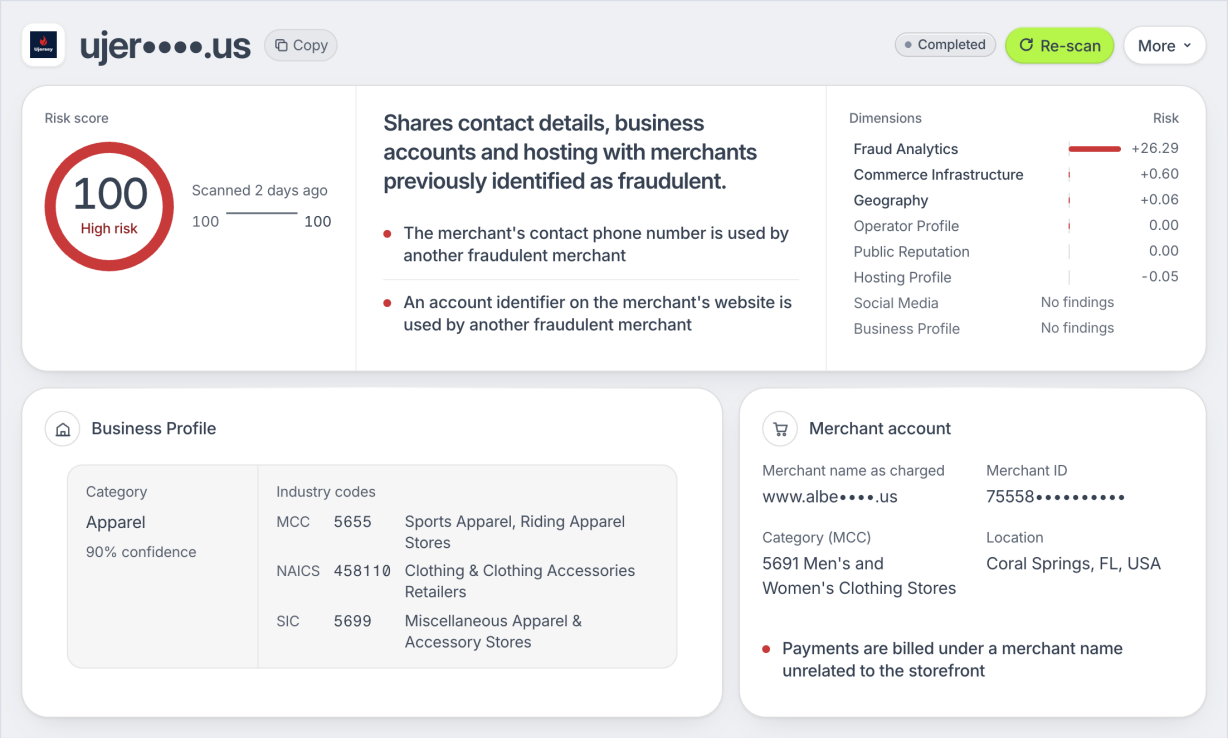


Figure 1. A storefront from the counterfeit sportswear ring, with the merchant account it bills through. Details are masked.

04 / FIRSTLIGHT

New merchants, assessed within hours of going live

FirstLight monitors new websites automatically as they come online.

Within hours, it links any storefront that shares an account, tracking identifier or contact detail with a merchant already rated high risk, often before that storefront has applied for a merchant account.

Every storefront is time-stamped when it is discovered and again when it is assessed, and each link carries a confidence level and a strength score.

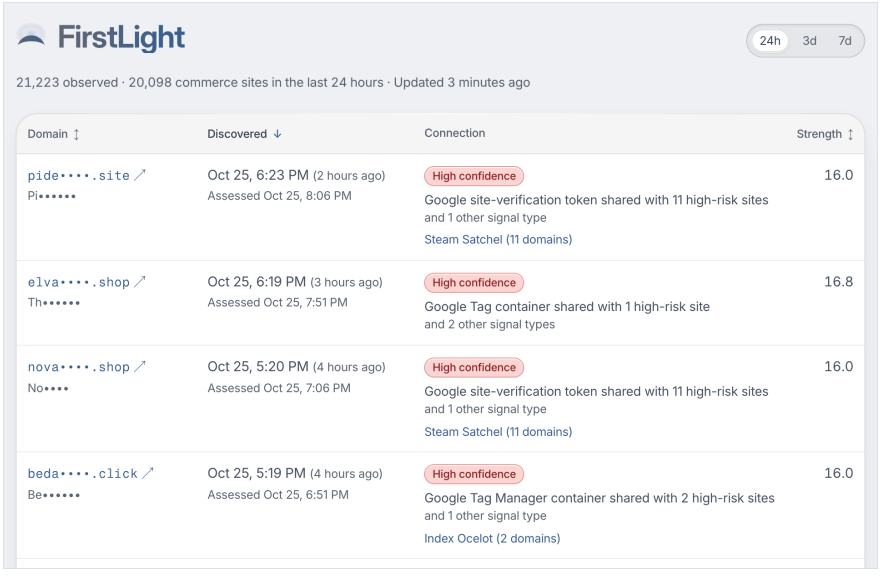


Figure 2. New storefronts discovered in the past 24 hours, each assessed and linked to a high-risk merchant within hours. Domains are masked.

05 / FRAUD RINGS

Fraud rings, mapped automatically

OneRisk links merchants through the identifiers their operators reuse, including contact emails and telephone numbers, payment and analytics accounts, and hosting infrastructure. Linked merchants are grouped into fraud rings and risk-rated as a single network. Each ring is monitored continuously, and a new storefront that carries any of its identifiers is attributed to it as soon as it appears.

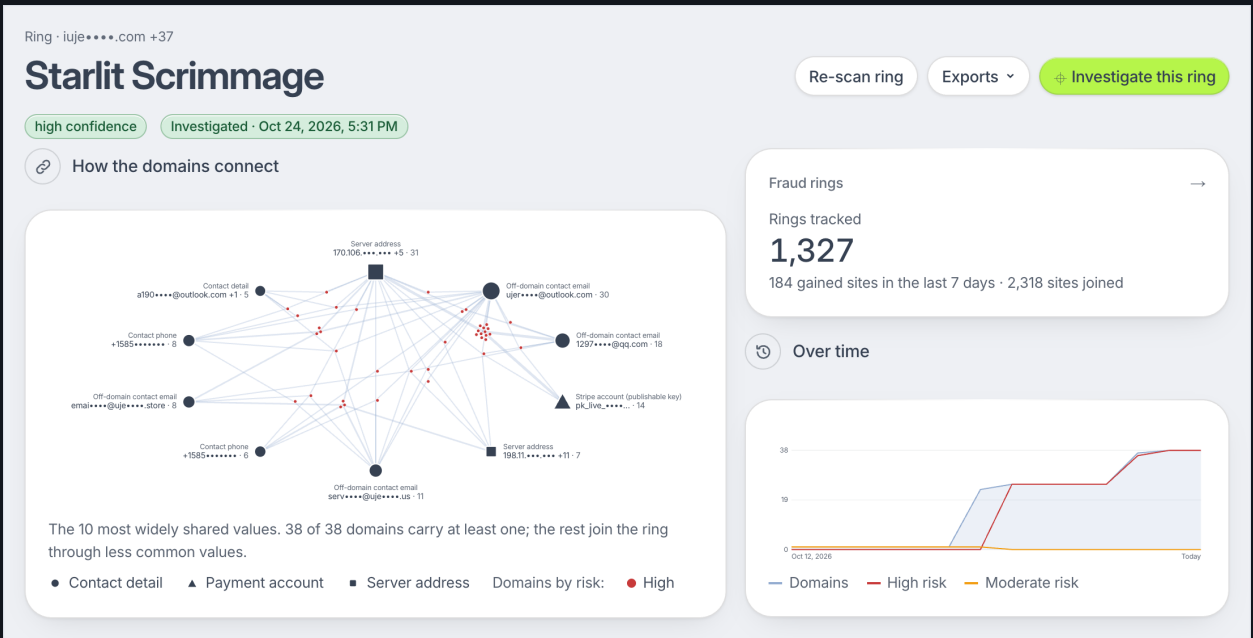


Figure 3. The counterfeit sportswear ring in OneRisk: the shared identifiers that link its storefronts, and the ring's growth. Details are masked.

06 / INVESTIGATE WITH AI

From a single lead to the operator behind it

Investigations start from a single website, email address or telephone number, whether it comes from a chargeback dispute, a card network alert or a suspicious applicant. OneRisk's AI pivots across domain registrations, contact details and analytics accounts, attributes the operator where public records allow, and packages the findings as an evidence report ready to share with processors and card networks.

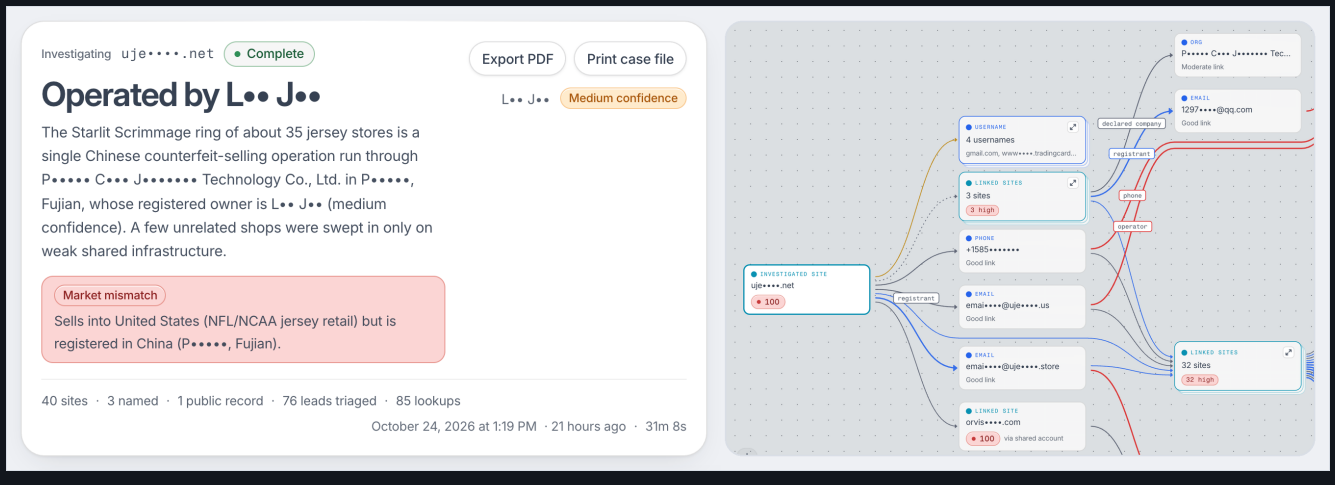


Figure 4. The case study's investigation: its conclusion, and the trail from the first storefront outward. Names are masked.

07 / PUTTING IT TO WORK

One platform across the merchant lifecycle

01 SCREEN YOUR PORTFOLIO

Find the fraud already in your portfolio

OneRisk assesses every merchant in your portfolio and identifies those that share contact details, accounts or an operator with known fraud anywhere online.

02 ONBOARD WITH CONFIDENCE

See the operator behind every applicant

Submit applicants by API or through the platform and receive a risk rating with reason codes, covering every site the operator runs, disclosed or not.

03 MONITOR CONTINUOUSLY

Know when a merchant's risk changes

OneRisk reassesses each merchant automatically on the schedule you set, alerts your team when risk rises, and attributes new storefronts to known fraud rings as they appear.

08 / PROVEN IN THE FIELD

Case study: a counterfeit sportswear ring

In October 2026, OneRisk linked a network of online stores selling counterfeit NFL jerseys to a single operator. None processed payments under its own name: sales were routed through merchant accounts registered to other businesses, a practice known as transaction laundering. Census had already identified every storefront, and an AI-led investigation attributed the ring to the company behind it.

8
MERCHANT ACCOUNTS BILLING FOR THE RING

6
BUSINESSES HOLDING THOSE ACCOUNTS

12 days
FROM FIRST FLAG TO THE COMPANY BEHIND IT

< 1 min
TO PRODUCE THE 49-PAGE EVIDENCE REPORT

HOW ONERISK IS DELIVERED

Web platform

Portfolio dashboard, merchant profiles, fraud rings and investigations.

API and webhooks

Synchronous or asynchronous assessments, with webhook delivery into your onboarding flow.

Evidence reports

Merchant and fraud ring reports ready to share with processors and card networks.

Reason codes

Every risk rating is supported by reason codes and evidence.

See what we see

Contact OneRisk to arrange a portfolio screen, an assessment of your onboarding pipeline, or a demonstration of the Fraud Ring Evidence Report. The full case study is available on request.

onerisk.com

About OneRisk

OneRisk is a merchant risk intelligence platform built on continuous coverage of every active online merchant. Acquirers, payment facilitators and ISOs use it to screen portfolios, underwrite applicants, monitor merchants and investigate fraud, with every risk rating supported by reason codes and evidence.

Figures are OneRisk records as of October 25, 2026. Time to link runs from when a new storefront is discovered to when it is linked to a known fraudulent merchant. Case study figures cover October 4–24, 2026. Screens are from the OneRisk platform, with identifying details masked.