

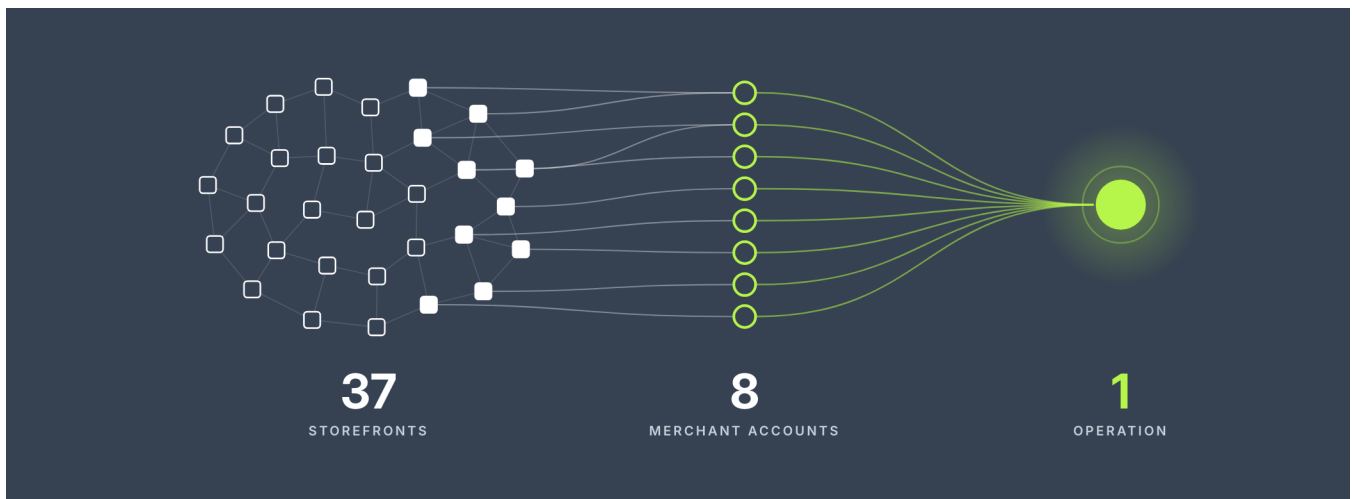


## CASE STUDY

# Taking down a counterfeit sportswear ring

How OneRisk connected 37 storefronts to one operation, traced their card payments to eight merchant accounts held in other businesses' names, and assembled the evidence a processor needs to act.

BY OneRisk Intelligence | October 2026



## 01 / OVERVIEW

# Executive summary

In October 2026, OneRisk uncovered a network of 37 online stores selling counterfeit NFL jerseys to U.S. shoppers. None of the stores processed payments under its own name. Instead, their sales ran through eight merchant accounts registered to six different businesses in three states, a practice known as transaction laundering. OneRisk identified the full network using Census, which holds intelligence on every active online merchant, together with AI that analyzes each merchant and uncovers hidden links between sites through advanced open-source intelligence gathering. An AI-led investigation then traced the operation to a technology company registered in Putian, China.

## Key takeaways

- **The store a cardholder pays is not the business an acquirer approved.** All ten storefront checkouts OneRisk examined billed under another business's name.
- **Internet-wide data exposes the whole network.** Census, OneRisk's index of more than 22 million online merchants, already held every storefront in the ring, so one shared contact address led to 30 of them.
- **AI does an analyst's reading at internet scale.** AI reviews each storefront's pages, legal terms and brand, and leads the AI-assisted investigation that traces who is behind them.
- **Rings keep growing, so detection has to keep pace.** The operator was still registering domains in September 2026, and OneRisk rated twelve newly attributed storefronts high risk within five minutes.

## At a glance

|                              |                                               |                                            |                                                                 |
|------------------------------|-----------------------------------------------|--------------------------------------------|-----------------------------------------------------------------|
| <b>37</b>                    | <b>8</b>                                      | <b>108</b>                                 | <b>22M+</b>                                                     |
| <b>STOREFRONTS</b>           | <b>MERCHANT ACCOUNTS</b>                      | <b>REPORTS OF HARM</b>                     | <b>MERCHANTS IN VIEW</b>                                        |
| Linked to a single operation | Billing for the ring under six business names | Public pages naming the ring's storefronts | Online merchants in Census, which already held every storefront |

Source: OneRisk records for the ring designated Starlit Scrimmage, October 4–24, 2026; Census total as of October 24, 2026.

## 02 / THE SCHEME

# Counterfeit storefronts on borrowed merchant accounts

Transaction laundering lets a merchant that could never pass underwriting accept cards anyway, by running its payments through a merchant account that belongs to another business.

## What shoppers saw

The ring's storefronts were built around the names "ujersey" and "jerseys." They sold replica jerseys for NFL, NBA, MLB and NHL teams from about \$40, some under banners claiming official merchandise, priced in U.S. dollars with U.S. telephone numbers and support offered over WhatsApp. Eight domains named for individual NFL teams were registered on the same day in November 2025, and sixteen storefronts reused a single holiday template.

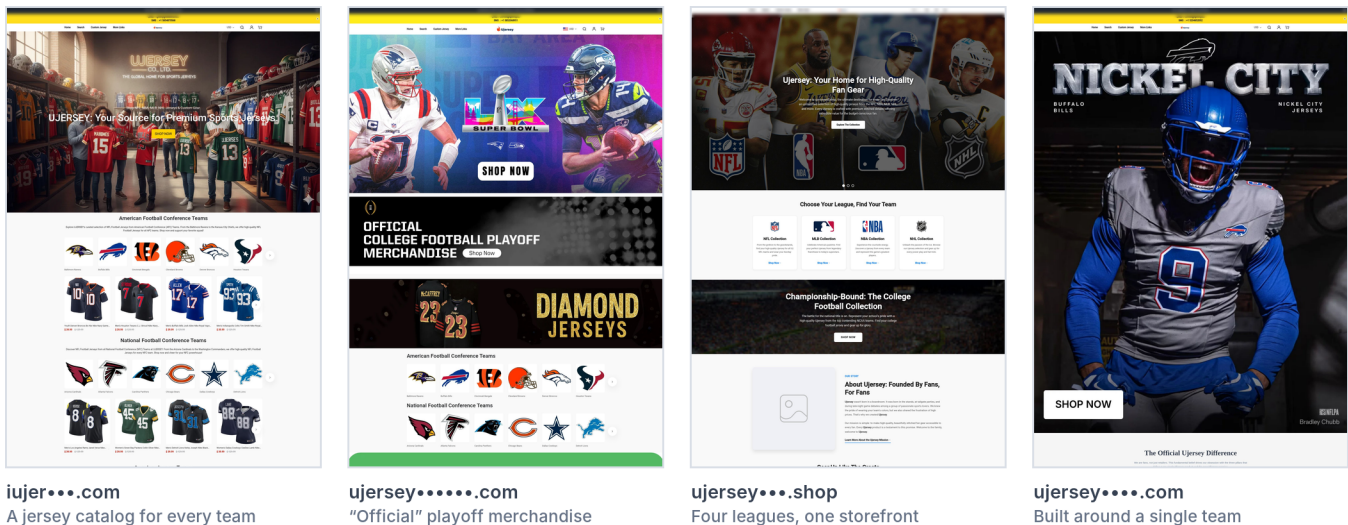


Figure 1. Four of the ring's storefront designs as OneRisk captured them.

## What the acquirers saw

Nothing that named the stores. Each of the ten checkouts OneRisk examined passed the card to a merchant account registered to another business, in Coral Springs and Casselberry, Florida; San Diego and Elk Grove, California; and Clearfield, Utah. Every account carried an ordinary clothing category code, so the ring's sales looked like routine apparel transactions to the acquirers that processed them.

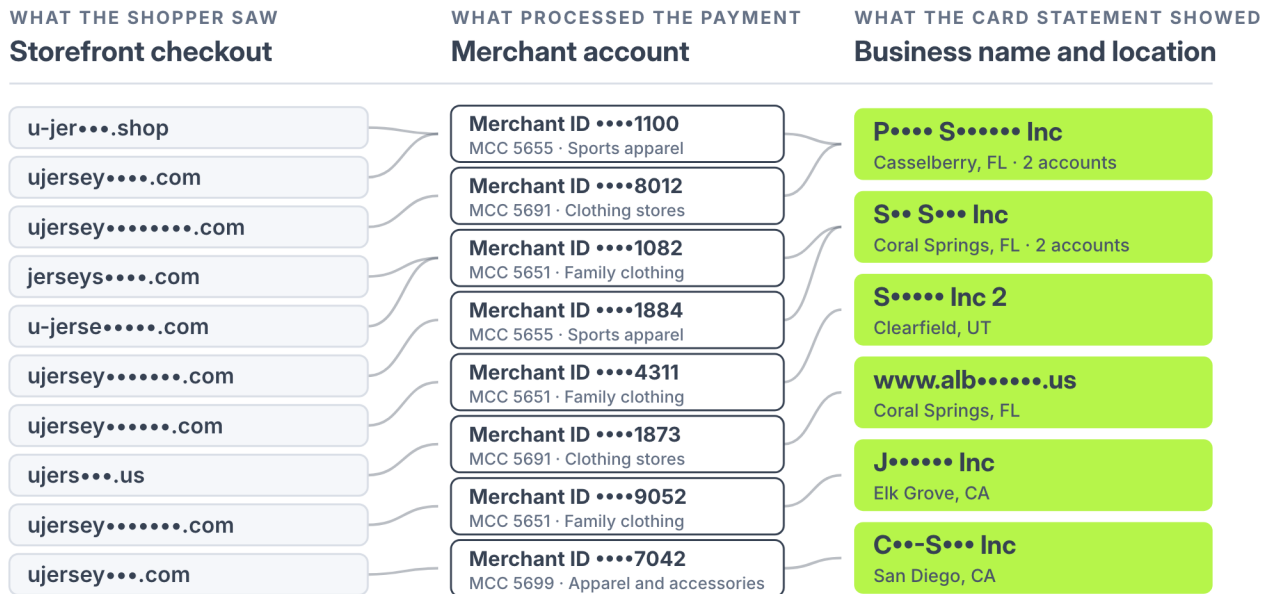


Figure 2. Ten storefront checkouts, eight merchant accounts, six businesses, with names as they appeared on the card statement.

The storefronts never apply for a merchant account, so onboarding checks never see them, and the businesses that hold the accounts look legitimate on paper. The only way to connect the two is to start from the storefront and follow the payment.

## The harm to cardholders

OneRisk found 108 public reports naming 32 of the storefronts on TikTok, the Better Business Bureau's Scam Tracker, PissedConsumer, Trustpilot and Reddit, the earliest dated September 2024. Shoppers describe counterfeit or poorly made jerseys, wrong sizes, missing orders, and refunds refused in favor of store credit.

## 03 / EVIDENCE

# The network, mapped

OneRisk links storefronts through the details they share. In this ring, those details were dense and specific to the operator.

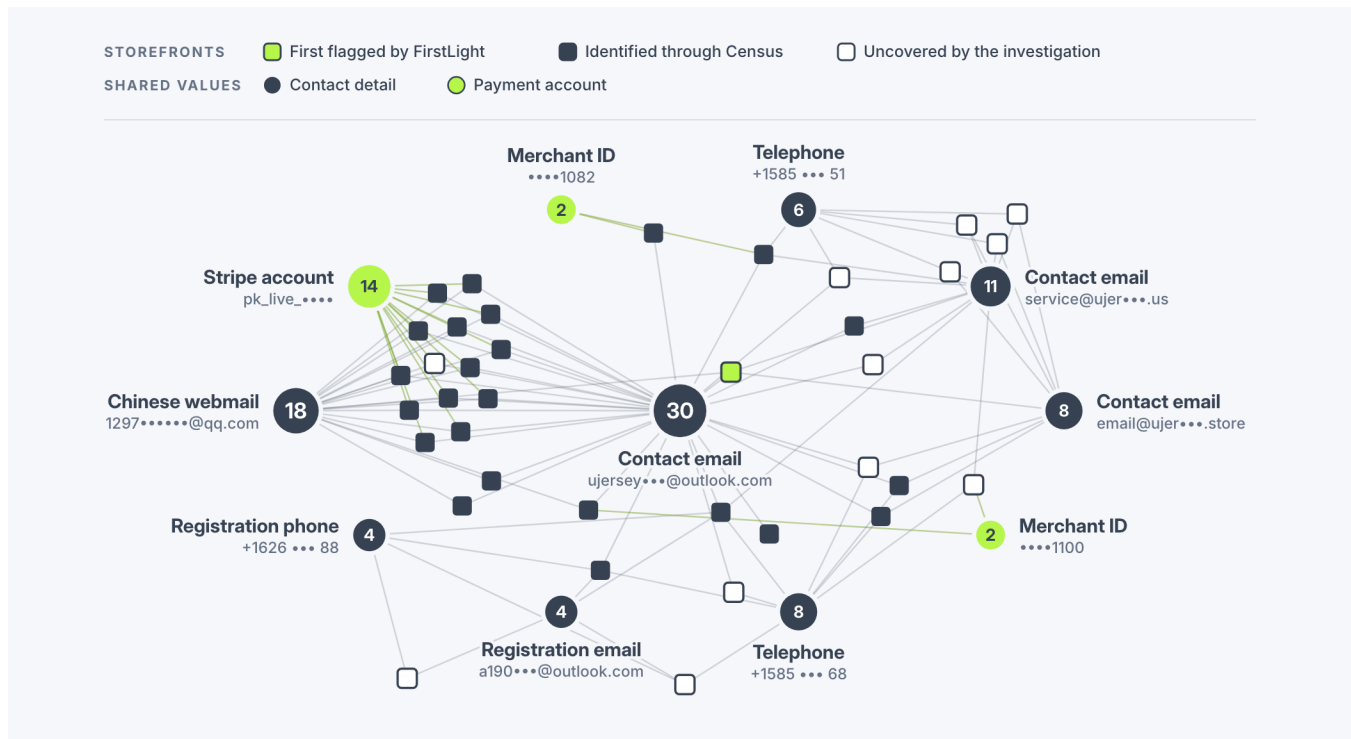


Figure 3. The ring as OneRisk maps it: 37 storefronts and the values they share.

The contact email address at the center of the map appeared on 30 storefronts and a Chinese webmail address on 18; further mailboxes, telephone numbers and a Stripe account used by 14 tie in the rest. In all, 36 of the 37 storefronts carry two or more shared values: one operation, not 37 unrelated merchants.

## Visibility across the internet

Screening that starts from one acquirer's portfolio sees only the merchants it has onboarded. Census covers every active online merchant, more than 22 million today, so a value found on one storefront can be traced to every site on the internet that carries it. Census has linked more than 137,000 merchants to known fraud this way, including 35 of this ring's 37 storefronts.

| SHARED VALUE                               | KIND                   | STOREFRONTS |
|--------------------------------------------|------------------------|-------------|
| ujersey•••@outlook.com                     | Contact email          | 30          |
| 1297•••••@qq.com                           | Chinese webmail        | 18          |
| pk_live_••••                               | Stripe payment account | 14          |
| service@ujer•••.us and email@ujer•••.store | Contact emails         | 11 and 8    |
| +1 585 ••• ••68 and +1 585 ••• ••51        | Telephone              | 8 and 6     |
| Six server addresses at Tencent Cloud      | Hosting                | 31 each     |

Table 1. The values that tie the ring together, by the number of storefronts that carry each.

## The reasons behind each rating

Every storefront received a risk score with the reason codes behind it; together they rated all 37 high risk.

| REASON IN THE ASSESSMENT                                                       | STOREFRONTS |
|--------------------------------------------------------------------------------|-------------|
| The merchant's off-domain contact email is used by another fraudulent merchant | 36          |
| The merchant's website shares an operator with domains confirmed as fraud      | 35          |
| The website is hosted on a network repeatedly used by fraud campaigns          | 31          |
| The website's page structure closely matches merchants already rejected        | 17          |
| The legal pages name a different company from the merchant's brand             | 17          |
| The legal pages contain unfilled template placeholders                         | 18          |
| Payments are billed under a merchant name unrelated to the storefront          | 8           |
| The website is a visual copy of another brand's website                        | 4           |

Table 2. Selected reasons from the ring's current assessments.

## 04 / CASE STUDY

# Starlit Scrimmage

From the first flagged storefront to the company behind it in twelve days, with each part of the OneRisk platform building on the one before.

## SECTOR

Counterfeit sports apparel sold to U.S. shoppers

## SCOPE

37 storefronts, 8 merchant accounts, 6 billing businesses

## TIMEFRAME

October 4–24, 2026

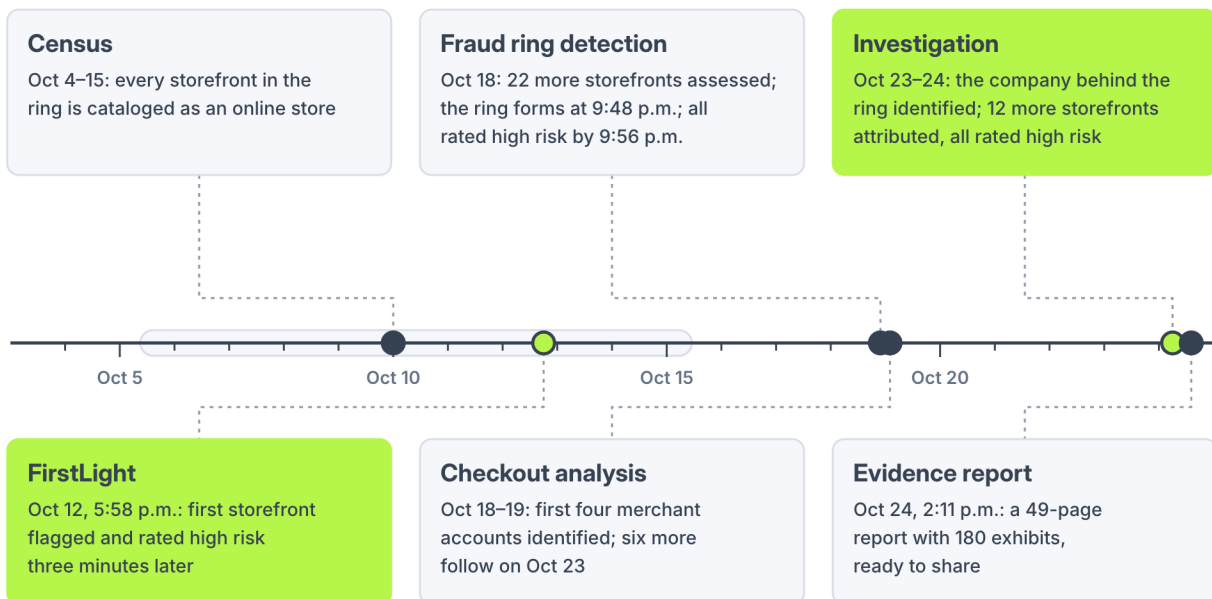


Figure 4. How the case developed, October 4–24, 2026 (Eastern Time).

## The challenge

The ring had been operating since at least 2024, yet none of its storefronts held a merchant account in its own name. Each site presented itself as a small, independent apparel retailer. The businesses that held the accounts were registered under ordinary clothing categories, and evidence of consumer harm was scattered across social media posts and review sites that could be removed at any time.

## The approach

### **Census: every storefront already on file**

Census, OneRisk's continuously updated index of active online merchants, uses AI to judge whether each website is a store. It had detected all 37 storefronts by October 15, before any was assessed.

### **FirstLight: the first flag**

FirstLight reviews websites as they come online in real time. On October 12 at 5:58 p.m., it flagged the first of the ring's storefronts, and OneRisk's full assessment rated it high risk three minutes later.

### **Merchant assessment and fraud ring detection**

On October 18, Census detected 22 more storefronts. OneRisk's AI agent reviewed each site's pages, legal terms and branding together with its hosting profile, and all 22 were rated high risk that same evening, each with the reasons behind its score (Table 2). At 9:48 p.m., OneRisk grouped the storefronts into a single fraud ring (Figure 3).

### **Checkout and payment analysis: following the money**

OneRisk identified the merchant account behind ten storefront checkouts: the business name, merchant ID, category code and location a card statement shows. They led to eight accounts held by six businesses, none named after the store (Figure 2); two businesses each operated two accounts.

### **Outside reports: evidence that survives deletion**

Of the 108 public reports of harm, OneRisk captured 30 pages as dated screenshots, so the evidence remains if a post is removed.

### **Investigation: the company behind the ring**

OneRisk's AI-led investigation began at the first flagged storefront and followed its registration emails and analytics accounts outward, examining 176 entities and 624 relationships across the network. The domain registrations listed a Japanese businessman and a California company as the owners, but neither was the real owner. The businessman's name also appears on the websites of genuine Japanese companies with no connection to the ring, which shows his identity was copied. The California company, formed in 2025, lists a home address shared by several other shell companies, and no business operates there.

The registrations also carried a Chinese webmail address and the name and street address of a technology company in Putian, in China's Fujian province. China's business registry lists that company at the same address, public records link the company's registered telephone number to the account behind the ring's Chinese webmail address, and one of the storefronts publishes that address alongside the ring's main contact email. Together, these links tie the storefronts to the company that runs them. A second AI review independently tested and confirmed the chain. The

investigations attributed twelve more storefronts to the ring, all rated high risk within five minutes, and set aside about 40 look-alike shops that shared only a widely used hosting address.



Figure 5. How the investigation traced the operator, from the first storefront to the company behind it.

## Fraud Ring Evidence Report: ready to share

One request produced the Fraud Ring Evidence Report: 49 pages and 180 numbered exhibits covering every storefront, the values that link them, the merchant accounts and the captured reports of harm, each summarized by AI and checked against its source, with file hashes and CSV data. It took less than a minute to prepare and is written for a payment processor to read without access to OneRisk.



By October 24 the ring was fully mapped, documented and traced to the company behind it. OneRisk continues to monitor it: a new storefront that carries any of its values is linked to the ring when it appears.

## 05 / RESULTS

## Results and impact

In twelve days, one flagged storefront became a fully documented operation traced to the company behind it.

| OUTCOME                 | RESULT                   | TIME           | CAPABILITY           |
|-------------------------|--------------------------|----------------|----------------------|
| First storefront rated  | High risk                | 3 minutes      | FirstLight           |
| Network identified      | 37 storefronts           | October 18–23  | Fraud ring detection |
| Merchant accounts found | 8 accounts, 6 businesses | October 18–23  | Checkout analysis    |
| Reports of harm         | 108 found, 30 captured   | By October 24  | Outside reports      |
| Storefronts attributed  | 12, all high risk        | October 23–24  | Investigation        |
| Operator identified     | Company in Putian, China | October 24     | Investigation        |
| Evidence package        | 49 pages, 180 exhibits   | Under a minute | Evidence report      |

Table 3. What OneRisk established about the ring, and how long each step took.

### What the results mean

For the acquirers behind the eight merchant accounts, the findings expose counterfeit sales through storefronts their merchants never disclosed. For card networks and processors, the evidence report sets out the storefronts, their links and the accounts that billed for them, ready to act on.

### Recommendations

1. **Start from the storefront, not the application.** An applicant's own website cannot reveal the storefronts that route payments through its account.
2. **Compare what the cardholder sees with what the statement shows.** A billing name or location that does not match the storefront is a direct indicator of transaction laundering.
3. **Treat linked storefronts as one risk.** An account that serves one storefront in a ring is exposed to all of them, and the ring will keep adding more.

## 06 / NEXT STEPS

## Conclusion

Transaction laundering works by keeping the storefront that takes the customer's money apart from the business that holds the merchant account. With data on every active online merchant and AI applied at every step, OneRisk puts them back together, from the first storefront to evidence a processor can act on.

### See what we see

Contact OneRisk to see how the platform assesses your merchants and the storefronts behind them, or to request a demonstration of the Fraud Ring Evidence Report.

### About OneRisk

OneRisk hunts fraudulent merchants by maintaining data on all active online merchants on the internet. New merchants, both legitimate and fraudulent, are detected within 90 minutes of coming online. Detect fraudulent merchants and monitor your portfolio for risk.

### Sources and methodology

1. OneRisk records and Fraud Ring Evidence Report for the ring designated Starlit Scrimmage, October 4–24, 2026.
2. OneRisk investigations of the ring, October 23 and 24, 2026, drawing on public business and domain registration records.
3. Public reports of harm on TikTok, the BBB Scam Tracker, PissedConsumer, Trustpilot and Reddit, as captured by OneRisk.

Figures are OneRisk observations, not estimates of the ring's sales or losses. Identifying details are partially masked; times are Eastern Time. Storefront screenshots are reproduced as evidence of the sites' content; no affiliation with any brand shown is implied.