

# Mixed-Mode Fraud Defense

Combining IP, Device, and Behavioral Signals in a Retail Omnibus

How Layered Detection Caught 34% Fraud

Blanc Research | December 2025

# The Omnibus Vulnerability

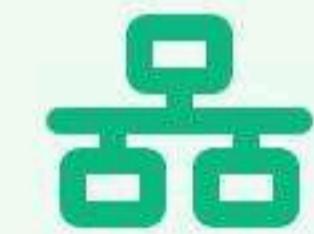
---

## High Volume, Mixed Sources, High Risk

- ✓ **Project Scope:** 12 product categories across 8,000+ respondents via multi-modal fielding (Panel, App, SMS).
- ✓ **The Problem:** Single-layer detection (IP-only) missed **68%** of contamination.
- ✓ **False Positives:** Legacy systems rejected 12% of legitimate respondents.
- ✓ **Business Stakes:** Flawed insights risked **\$1.2M annually** in misguided inventory and promo decisions.



# Three-Signal Defense Framework



## 1. IP Intelligence

Detects duplicate IPs, VPNs, and geolocation mismatches.

*Limitation:* Often blocks legitimate shared networks and is easily bypassed by residential proxies.



## 2. Device Fingerprinting

Captures hardware signatures, OS versions, and screen resolutions.

*Limitation:* Can miss sophisticated spoofing or flag legitimate users on multiple devices.



## 3. Behavioral Analytics

Monitors response timing, mouse entropy, and attention consistency.

*Limitation:* Advanced bots can mimic patterns; legitimate power-users may trigger alerts.

**The Solution:** Combine all three signals – fraudsters rarely fool all three simultaneously.

# Real-Time Detection & Scoring

$$\text{Risk Score} = 0.35 \times \text{IP}_{\text{Risk}} + 0.30 \times \text{Device}_{\text{Risk}} + 0.35 \times \text{Behavioral}_{\text{Risk}}$$

Threshold:  $>0.65$  = Auto-Pause |  $0.45-0.65$  = Review Queue |  $<0.45$  = Accept



- **Green (Clean): 66% (5,280 responses)**
- **Yellow (Review): 23% (1,840 responses)**
- **Red (Blocked): 11% (880 responses)**

*Key Win: 34% total fraud identified with only 3% false-positive rate.*

# Signal-by-Signal Impact

## IP Signal

### Caught:

- ✓ 340 duplicate IPs
- ✓ 560 Proxy/VPNs
- ✓ 320 Geolocation Mismatches

**Accuracy: 68%**

## Device Signal

### Caught:

- ✓ 480 Identical Fingerprints
- ✓ 210 Impossible OS Combos
- ✓ 140 Resolution Clusters

**Accuracy: 71%**

## Behavioral Signal

### Caught:

- ✓ 860 Straight-lining
- ✓ 520 Impossibly Fast
- ✓ 340 Zero-variance Timing

**Accuracy: 84%**

Signal overlap revealed **980 responses** failing 2-3 signals simultaneously.

# Business Impact & Outcomes

---



- ✓ **Data Quality:** Reduced fraud contamination from 34% down to **2% residual noise**.
- ✓ **Metric Shifts:** "Organic" preference dropped from 68% to 42%, aligning with reality. Price sensitivity threshold moved from \$15 to \$22.
- ✓ **Strategic Corrected:** Adjusted shelf allocation and increased online fulfillment capacity by 18 units/week.
- ✓ **ROI Realized:**  
**\$1.2M avoided** in misguided strategy.  
**\$340K saved** in wasted incentives.

# Building Resilient Omnibus Research

## Key Lessons & Best Practices

- ✓ **Layer Signals:** Single-signal leaves 30%+ fraud undetected. Mixing is non-negotiable.
- ✓ **Real-Time Scoring:** Prevents quota pollution better than post-field cleaning.
- ✓ **Weighting:** Use 0.35/0.30/0.35 (IP/Device/Behavioral) for optimal balance.
- ✓ **Thresholds:** Adjust per mode—Mobile App needs stricter rules than Panels.

## Scaling & Call to Action

- ✓ **Deploy Everywhere:** Extend to all omnibus tracks and custom projects >500 respondents.
- ✓ **Measure ROI:** Track fraud caught vs. sample cost savings quarterly.

### Action Item:

*"Don't defend with one signal—layer IP, device, and behavior into your fraud prevention arsenal."*

Blanc Research