Rysun
infinite possibilities

www.rysun.com

E-COMMERCE **FRAUD PREVENTION** FOR RETAILERS

The Fraud Landscape at Peak Shopping Periods

As U.S. online retail accelerates during peak shopping periods, so does fraud risk. In the 2024 holiday season window (Thanksgiving through Cyber Monday), ***4.2 % of attempted U.S. e-commerce transactions were suspected of digital fraud,*** underscoring persistent exposure during high sales events.

Retailers face a dual challenge: protecting revenue and preserving customer trust even as fraudsters use automated attacks, identity abuse, and chargeback exploitation to scale losses.

Key drivers include:

- **Massive transaction spikes** that conceal fraudulent activity
- **Consumer urgency,** leading to reduced vigilance
- **Higher financial stakes,** with revenue concentration in Q4
- **Rapidly evolving fraud tactics** including bots, automation, and identity spoofing
- **Post-season dispute surge,** with January–February seeing the highest chargeback volumes

Types of E-Commerce Fraud

Card-Not-Present (CNP) Fraud

Stolen card data used at checkout; spikes sharply on peak sale days.

Account Takeover (ATO)

Fraudsters exploit high login/signup activity to access stored cards, loyalty points, and saved addresses.

Synthetic Identity Fraud

Fake accounts created using blended real or fabricated credentials, often used to exploit BNPL or promotions.

Friendly Fraud / Chargeback Abuse

Legitimate customers dispute valid purchases after the busy shopping period.

Return & Refund Abuse

Wardrobing, empty-box returns, and excessive return manipulation in January–February.

Ad & Affiliate Fraud / Fake Sites

Look-alike sites, bot-driven ad clicks, and coupon exploitation during aggressive holiday promotions.

Prevention Strategies & Controls

- **Real-Time ML/AI Detection**

  Use adaptive models to handle peak traffic, catch unusual behavior, and reduce manual reviews.

- **Stronger Identity Verification**

  Device fingerprinting, behavioral biometrics, MFA, and verification layers for new accounts and high-risk orders.

- **Bot & API Protection**

  Rate limiting, bot detection, and traffic scoring across APIs, mobile apps, and checkout flows.

- **Returns & Chargeback Management**

  Return-reason analytics, refund holds on high-risk items, and post-holiday dispute monitoring.

- **Ad & Affiliate Safeguards**

  Monitor invalid traffic, vet affiliates, and track impersonation attempts across domains/social ads.

Top 5 Best Practices for Retail Decision-Makers

1. **Plan Early & Cross-Functionally**
   Integrate fraud strategy with marketing, supply chain, and customer-experience planning.

2. **Tune Controls for Peak Conditions**
   Adjust thresholds, scoring models, and approval/decline logic specifically for surge periods.

3. **Segment Customers by Trust**
   Offer low-friction checkout for trusted profiles while tightening risk controls for unknown/new users.

4. **Monitor the Full Customer Journey**
   Track fraud signals from login → checkout → delivery → returns → disputes.

5. **Prepare a Post-Holiday Fraud Playbook**
   Review January–February chargebacks, refine models, and feed insights into next year's fraud strategy.

What Success Looks Like: Industry Benchmarks

Here is a concise set of benchmarks and key performance indicators (KPIs) that senior decision-makers can use to evaluate the effectiveness of their fraud prevention program. These are grounded in industry-recognized rates and standards drawn from publicly reported fraud metrics and industry research.

Goal	Metric	Benchmark / Reference	What Success Looks Like
Minimize chargebacks	Chargeback rate	Average e-commerce chargeback rate ≈ 0.6 % ***(avoid exceeding 0.9 %to prevent penalties)***	Maintain ≤ 0.9 % chargeback rate while scaling volume
Reduce fraud occurrence	Fraud rate	Holiday fraud flagged ***~4.2 % of attempted transactions***	Fraud-rate below seasonal peak benchmarks (e.g., below prior year peak)
Maximize true approvals	Approval rate	Rate varies; strategic KPIs include acceptance above 75 % with low fraud	High approval rates with low fraud exposure
Limit manual impact	Manual review volume	Best practice is to scale automation; manual review ideally <10–15 % of orders	Minimal manual reviews, with high-confidence risk automation
Detection quality	False positives/ precision	KPI frameworks suggest ***balancing fraud detection vs false declines***	Low false positives (false declines minimized) while catching fraudulent transactions