Player Behavior Fraud Pattern Detection Case Study

Author: Vincent Wilkinson Jr.

---

1. Executive Summary

This case study shows how I identify suspicious player behavior, fraud patterns, and operational risks on a fantasy sports/gaming-style platform. I will be Using a fictional dataset of current and retired nba and nfl players I created myself, breaking down behaviors such as:

- device sharing
- multi-accounting
- withdrawal abuse
- stale line hunting
- shadowing sharp accounts
- injury-window exploitation

The goal of this project is to demonstrate real pattern recognition, timing awareness, and operational decision-making. It is also to show recruiters that I understand the process and the looks of a good case study can talk to it. I am very coachable and a fast learner.

---

2. Dataset Overview

The dataset includes 30 fictional users with realistic activity patterns:

- timestamps
- stakes

- sports (NBA/NFL)
- entry types (Flex/Power)
- device IDs
- locations
- user notes and indicators

I intentionally mixed:

- normal users
- sharp players
- opportunistic bettors
- promo hunters
- abuse patterns
- suspicious device clusters

This simulates the type of real cases a Fraud or GameOps analyst monitors daily.

---

3. Key Fraud & Behavior Patterns Detected

A. Withdrawal Abuse

Users **U102** and **U910** repeatedly:

- win
- instantly withdraw
- return only when the balance hits zero

This typically signals:

- bonus abuse
- account cycling
- hit-and-run style play
- reduced platform engagement

B. Device Sharing / Multi-Accounting

Examples:

- U188 & U511 (same device)
- U502 & U503
- U300 & U301

This behavior may indicate:

- multiple accounts to bypass limits
- shared devices across several users
- coordinated play

C. Injury-Window Exploitation

Users **U311** and **U147** enter plays **within minutes** of public injury news.

This is usually sharp timing behavior:

- backup overs
- substitute player value spots
- real-time market reactions

- exploiting stale projections

D. Stale Line Hunting

User **U220** consistently finds mispriced lines *before* the board adjusts.

User **U912** shadows U220's entries within seconds.

This shows:

- stale-line exposure
- sharp → shadow pattern
- possible Discord/Telegram group picks
- fast market-reaction behavior

E. Location Mismatch

User **U444** logs in from GA and then AL within hours with no realistic travel gap.

This may indicate:

- GPS manipulation
- account sharing
- location spoofing

F. Sharp Shadowing

Sharp users get copied by smaller accounts:

- U150 → U151

- U900 → U901

This suggests:

- coordinated groups
- pick-copying behavior
- information sharing
- shared strategy patterns

---

4. Operational Thinking & Workflow

If I were on a Fraud or GameOps team, my approach would include:

- Tagging suspicious accounts based on behavior clusters
- Reviewing device fingerprints & IP groupings
- Monitoring timing patterns (injury, stale line windows)
- Escalating location mismatches
- Identifying sharp accounts and analyzing shadow followers(betting groups)
- Communicating with GameOps when lines need freezing or updating
- Tracking high-risk users for repeat behavior

---

5. Recommendations

To reduce risk and improve monitoring:

- Add device-cluster alerts for shared devices

- Introduce withdrawal cooldown logic for fast-exit accounts
- Improve stale line detection with quicker market sync
- Track sharp–shadow account relationships
- Require geo-verification for sudden location changes

---

6. Conclusion

This project shows my ability to put together a case study, and how I would identify:

- fraud indicators
- suspicious behavior
- sharp vs. coordinated patterns
- risk exposure
- timing exploitation
- device and location anomalies

I really do enjoy this work and I'm just building up a portfolio for recruiters to take a chance on someone hungry— spotting what most people overlook. I plan to continue building fraud, behavior, and operational case studies as well as others as I grow and demonstrate my skill set.

Thanks for your time.