Online Gaming Fraud Prevention Checklist

This checklist provides actionable steps to detect and prevent online gaming fraud. Use it to assess your current security measures and identify areas for improvement.

Risk Assessment & Planning:

- [ ] **Conduct a thorough risk assessment:**
    - Identify potential fraud types relevant (e.g., account takeover, payment fraud, bonus abuse).
    - Evaluate your current security measures and their effectiveness.
    - Assess the potential impact of fraud on your business (financial, reputational).
    - Prioritize vulnerabilities and develop a mitigation plan.
- [ ] Establish a fraud prevention team or designate responsible individuals.
- [ ] Set clear fraud prevention goals and objectives.
- [ ] Develop a communication plan for handling fraud incidents.

User Authentication & Access Control:

- [ ] Implement strong password policies (length, complexity, expiration).
- [ ] Enforce Multi-Factor Authentication (MFA) for all users, especially admins.
- [ ] Use CAPTCHA on signup and login forms to prevent bot activity.
- [ ] Implement role-based access control to restrict user permissions.
- [ ] Regularly review and revoke access for inactive or terminated users.
- [ ] Consider biometric authentication for added security.

Platform & Infrastructure Security:

- [ ] Implement a Web Application Firewall (WAF) to protect against web attacks.
- [ ] Use SSL encryption for all communication between users and your servers.
- [ ] Regularly update your software and server infrastructure to patch vulnerabilities.
- [ ] Conduct regular security audits and penetration testing.
- [ ] Encrypt sensitive data both in transit and at rest.
- [ ] Implement intrusion detection/prevention systems.
- [ ] Secure your APIs with proper authentication and authorization mechanisms.

Payment Security:

- [ ] Use a PCI DSS compliant payment gateway.
- [ ] Implement Address Verification System (AVS) and CVV checks for card transactions.
- [ ] Use 3D Secure authentication (e.g., Verified by Visa, Mastercard SecureCode).
- [ ] Monitor transaction patterns for suspicious activity (e.g., unusual amounts, multiple transactions from the same IP).
- [ ] Implement fraud scoring and risk-based transaction screening.

Data Enrichment & Monitoring:

- [ ] Implement IP geolocation to identify suspicious login locations.
- [ ] Use device fingerprinting to detect devices associated with fraudulent activity.
- [ ] Monitor user behavior (login patterns, in-app activity) for anomalies.
- [ ] Integrate with fraud prevention services for data enrichment and risk scoring.
- [ ] Set up alerts for suspicious activity (e.g., unusual login attempts, large transactions).
- [ ] Regularly review server logs for suspicious activity.

Collaboration & Partnerships:

- [ ] Partner with a reputable eCommerce provider specializing in video games fraud management.
- [ ] Stay informed about the latest fraud trends and techniques.

Employee Training & Awareness:

- [ ] Train employees on security best practices and fraud awareness.
- [ ] Educate employees on how to identify and report suspicious activity.
- [ ] Implement a security awareness program to keep employees informed.

Incident Response:

- [ ] Develop an incident response plan for handling fraud incidents.
- [ ] Establish clear procedures for reporting and investigating fraud.
- [ ] Regularly test your incident response plan to ensure its effectiveness.

Continuous Improvement:

- Regularly review and update your fraud prevention strategy.
- Analyze fraud incidents to identify areas for improvement.
- Stay up-to-date with the latest security technologies and best practices.