Dropfans.io – Chargeback & Fraud Mitigation Policy

Version: 1.0 **Last Updated:** 2025-12-31

1. Philosophy & Objective

Dropfans.io operates with a **Zero-Tolerance Policy** regarding fraud. Given the high-risk nature of digital content sales ("Drops"), our primary objective is to maintain a chargeback ratio well below the Card Brand monitoring thresholds (below 1%). We employ a proactive "Defense-in-Depth" strategy that prioritizes blocking fraudulent transactions before they occur over fighting disputes later.

2. Pre-Transaction Prevention

To prevent the entry of bad actors, we utilize the advanced security features of our payment partner combined with our own internal validation rules.

2.1 Authentication & Validation

- **3D Secure (3DS2):** We enforce 3D Secure challenges on transactions (particularly for EEA/UK traffic) to verify card ownership and shift liability.
- **AVS & CVV Matching:** All transactions require a strict match for the Card Security Code (CVV). Address Verification Service (AVS) checks are performed where applicable to ensure billing details match the cardholder's bank records.
- **Email Verification:** No user may transact without a verified email address confirmed via OTP (One-Time Password) or link.

2.2 Transaction Limits (AML Controls) To prevent money laundering and mitigate high-value losses, we enforce the following hard limits:

- **Maximum Single Transaction Limit:** “Drops” (Pay-Per-View) purchases are capped at **$1,000.00 USD** per transaction. Any attempt to process a higher amount is automatically declined to prevent money laundering and card testing.
- **Velocity Cap:** We do not impose a strict limit on the *number* of transactions per hour, acknowledging that legitimate users may unlock multiple "Drops" in succession. Instead, we rely on **Pattern Recognition** (see Section 3) to distinguish fans from bots.

3. Transaction Monitoring & "Whaling" Detection

We utilize real-time monitoring to flag suspicious behavior patterns while facilitating legitimate high-volume users.

3.1 Bot vs. Human Pattern Recognition We distinguish between "High-Spending Fans" and "Automated Scripts" based on purchasing speed:

- **Human Behavior:** We recognize that legitimate users often make multiple small purchases in short intervals (e.g., every 2-3 minutes). This is treated as normal behavior.
- **Bot Behavior (Inhuman Speed):** Accounts that attempt transactions at physically impossible speeds (e.g., multiple purchases per second or simultaneous unlocks) are immediately flagged, and the transactions are voided.

4. Post-Transaction Alerts & Deflection

We utilize industry-standard tools to resolve disputes before they become formal chargebacks.

4.1 Early Warning Systems

- **Ethoca & Verifi:** Dropfans.io actively utilizes **Ethoca Alerts** and **Verifi (CDR)** to receive real-time notifications of confirmed fraud or customer disputes from issuing banks.
- **Proactive Refunds:** To retain a low chargeback rate we may immediately refund the transaction to prevent the dispute from escalating into a formal chargeback.

5. Dispute Resolution & Consequences

5.1 "Friendly Fraud" Defense In the event of an illegitimate dispute (e.g., a user claiming "Item Not Received" after watching the content), we are able to submit a comprehensive evidence package **to the issuing bank or to our partnered payment provider, including**

- **Consumption Logs:** Timestamps proving the specific content was unlocked and viewed.
- **Device Fingerprinting:** IP address, Device ID, and location data at the time of purchase.
- **TOS Acceptance:** The digital timestamp of the user accepting our "Immediate Consumption" terms.

5.2 Banning & Blacklisting

- **Immediate Ban:** Any user confirmed to have engaged in fraudulent behavior (card testing, use of stolen cards) or who initiates a chargeback is **immediately and permanently banned**.
- **Blacklisting:** The user's credentials (Email, IP Address, Card Fingerprint, and Device ID) are added to our internal **Negative Database** to prevent them from creating new accounts.

6. Creator Payout Protection

To protect the platform and our payment partners from financial liability, we enforce strict payout rules for Content Creators.

6.1 Rolling Reserve & Hold Period

- **21-Day Payout Delay:** All Creator earnings are held in a "Pending" state for a period of **21 days** before being released for payout.
- **Purpose:** This window allows us to identify and process any potential fraud, alerts, or chargebacks *before* funds leave the platform.

6.2 Clawbacks

- If a transaction is refunded or charged back, the associated earnings are immediately deducted ("clawed back") from the Creator's pending balance. If the balance is insufficient, a negative balance is applied to future earnings.