CALIFORNIA GAMBLING CONTROL COMMISSION

GAMING POLICY ADVISORY COMMITTEE PRESENTS:

TPPPS BEST PRACTICES FOR THEFT PREVENTION

October 2026

TPPPS Theft Prevention: Operational Best Practices

The Gaming Policy Advisory Committee (GPAC) met through 2025 and 2026 to discuss best practices for the operation of Third-Party Providers of Proposition Player Services (TPPPS).

As a result of those discussions, GPAC developed this guidance to help TPPPS companies mitigate internal and external theft risks. These best practices focus on high-visibility deterrents, data-driven monitoring, and standardized operational controls and should be tailored to the unique operational and security needs of each TPPPS and Cardroom environment.

This guide is not an all-encompassing list, and is intended to help guide stakeholders in operations. Successful theft prevention requires a dynamic approach that evolves with new technology and emerging risks in the gaming environment.

If you have any questions about this TPPPS theft prevention resource or any other GPAC project, please email gpac@cgcc.ca.gov.

I. Training & Education

- **Asset Protection Fundamentals:** Educate appropriate team members on mitigation techniques and theft risks, including risks associated with chip handling, table-side behavior, and behavioral red flags.
- **Regulatory Compliance**: Educate appropriate team members on applicable gaming regulations regarding TPPPS operations.
- **Reporting Protocols**: Establishing a clear, anonymous "whistleblower" channel for reporting suspicious activity without fear of retaliation.

II. Table Monitoring & Session Analysis

- **Collusion Prevention**: Work to identify patterns where specific TPPPS players consistently lose during a specific house dealer's down, or to specific cardroom patrons, to the extent operationally feasible.
- **Outcome & Buy-in Variance**: **Win/Loss Analysis**: Monitor player outcomes to identify statistical anomalies that deviate from expected house edges, when appropriate.

TPPPS Theft Prevention: Operational Best Practices

III. Attire & Physical Controls

- **Apparel**: Implementing an operationally reasonable attire policy balancing asset security with other considerations, including comfort, affordability, and enforcement.
- **Design Modifications to Consider:**
  - ◊ **Pocket Elimination**: Removing all pockets or permanently sewing pockets shut to prevent the concealment of chips or currency.
  - ◊ **Outerwear Restrictions**: Prohibiting overly bulky outerwear (jackets, hoodies, or thick sweaters) that could easily hide gaming assets or equipment.
- **Personal Item Restrictions:**
  - ◊ Limiting personal items on the gaming floor to essential equipment only.
  - ◊ Prohibiting the use of personal cellular devices or smartwatches at the table.

IV. Accountability

- **Regular Financial Audits**: Conducting unannounced tray audits and chip counts mid-shift to ensure accuracy.
- **Employee Performance**: Utilize "Security and Asset Integrity" as a core metric in evaluating employee performance.
- **Podium and Chip Transport Security**: Establish procedures addressing podium and chip transport security for operational protection and theft prevention.

V. Surveillance & Auditing

- **Proactive Video Reviews**: Moving beyond "reactive" reviews (after a loss is reported) to "proactive" analysis leveraging emerging technology, including random audits of session play and other steps based on operational feasibility.
- **Close-Up Coverage**: Work with the cardroom to ensure coverage of the TPPPS chip tray and all hand-to-hand transactions.
- **Electronic Playbooks**: Implement electronic playbooks where operationally feasible.