# New Fraud Control Tool

Specification v1.0

## Table of contents

## Glossary

**Game Protocol** – internetworking protocol between the game server processing the game logic and the game client. The data sent by the game client and the response from the server can be viewed using sniffers.

**Hack** – in the context of this specification, it is a direct impact on game logic or server-side processing. It is possible only with an existing vulnerability using special tools.

**RTP (Return to player)** – a mathematical parameter of the game showing how much (in percentage) the game can payout to the player relative to his bets on an infinite number of bets. In most cases, the practical RTP of a game tends to the theoretical RTP only when calculated over a million or more rounds. Is computable, i.e., it is possible to calculate the deviation from the theoretical for any number of rounds.

**Progressive slots** – slot game in which player increases the progress during the game, performing certain actions (getting any combinations, or simply with each bet). The end of the progress gives the player any payouts, bonus rounds, etc. (depending on the rules of the game).

**SD (Standard deviation)** - measure of the amount of variation or dispersion of a set of values. In the context of this specification, these are the possible limits on the deviation of the RTP from what is expected for a given number of rounds.

**Strategy** – in the context of this specification, this is a set of actions within the game that any player can perform without third-party software and get a profit (RTP is higher than the theoretical one).

**TBD** – to be determined later.

**TJD** – BSG game «Triple Juicy Drops».

**TTB** – BSG game «Take The Bank» and clones «Take Santa’s Shop» and «Wild Cherry Blast» (NG game).

## Overview

New fraud control tool is a program that should help to quickly respond to possible game vulnerabilities, system hacks, as well as the presence of strategies in games.

The main goal of this program is to analyze the gaming activity of all games and players, as well as to instantly react and perform certain actions in case of detection of suspicious activity.

Analysis of gaming activity should be carried out according to predetermined criteria. The criteria should be designed in such a way as to determine the deviations of the RTP from the theoretical one, as well as to check the game activity for previously identified hacks and strategies.

## 1.1 Previous issues

### 1.1.1 Take The Bank issue

In this game, after the release, a bug was found in the form of the ability to use a strategy and influence the final progress.

When changing the bet, the progress of the current bet was reset. Several rounds from the start of the progress could affect the final payment for the progress. Thus, the players made several bets from the beginning of the progress, and if they were satisfied with the initial progress values, they continued to play until the end of the progress, otherwise they changed the bet and started progress on a new bet (on the previous bet, the progress was reset at that time). Thus, the players played only on the "correct" progress, which brought more income and increased the RTP of the game in favor of the player.

This bug has the following characteristics:

- The player played a lot only in this game (many gamesessions).
- The RTP of the game for a player on a specific number of rounds is above the variance rate.
- In sessions, a frequent change of coins was found.

The bug fix was to save the progress for each coin separately without the possibility of resetting.

### 1.1.2 Triple Juicy Drop issue

In this game, after the release, a bug was revealed with the abuse of progress using multi-accounting.

The frequency of combinations with certain symbols was higher than the frequency of combinations with the rest. At the beginning of the progress, some symbols are selected by collecting which, during the progress, you can get a chance to big payout. Progress for each coin is different.

The players used the knowledge about the different frequency of different symbols falling out, and if at the beginning of the progress the game chose a favorable symbol, then the players continued the game. Players also tested game-selected symbols for progress on different coins. They also used a casino vulnerability that allows creating multiple accounts with different currencies for an account with one wallet. Thus, using several accounts, players played only those bets for which there was initially a favorable win forecast (forecast abuse).

For this game, 1.1.1 issues have been fixed, however multi-accounting has allowed progress to be abused. And this approach also influences many progressive games. Using multi-accounting for a casino account with one wallet (for our system different accounts for each currency) players can abuse progress by choosing a favorable beginning of progress.

Indirect signs:

- One player played only one game for several sessions (small number) at different stakes.
- Possibility on the side of the casino to play for several currencies (for us – different accounts). It is impossible to determine on our side.
- With a small number of sessions RTP is always >100%. Usually within normal limits, but in conjunction with only one game and a small number of sessions, it can be an indirect sign.
- A large number of "such accounts" on the bank.

The fix for this problem is the revision of the mathematical model.

### 1.1.3 Table games issues

In contrast to the use of strategies in progressive slots, in Table games issue mainly used vulnerabilities in the protocol between the client and the server.

In several previous issues, the following hacks were used:

- Changing the data in the request from the client to the server and resending it. Usually, the data was changed in such a way as to break the protocol. That is, extra values or incorrect values.
- Repeated negative bet requests for a game that supports such functionality (Ride’m Poker).

Distinctive signs of such hacks:

- VBA bet values are incorrect (0 or negative values).
- High RTP by sessions.

## 1.2 General Signs of Abuse

Based on sections 1.1.1-1.1.3 the main difference between games in which players abused progress or used hacking is the high RTP of the game per player, as well as gamesessions of only one game.

Also, one of the criteria for the presence of an indefinite vulnerability may be the presence of a large number of accounts on the bank playing only one game and having an RTP > 100% (or having played several times and never logged in again).

Frequent change of Bet in a gamesession can also be used as one of the set of criteria for determining the abuse of the game.

## 1.3 Current Tools

### 1.3.1 Fraud control

A tool that allows to monitor the RTP of the game for the corresponding player and send an email notification in case the RTP deviates from the pre-set criteria.

That is, for the bank on which this monitoring is activated, 3 criteria can be set for each game.

Each criterion contains:

- Interval of rounds (min-max).
- The maximum RTP of the game for the given interval.

Thus, there are 3 intervals with corresponding maximum possible RTPs. To exclude false positives, the minimum number of game rounds for a player (for a specific game) must be 10,000. The same value is the minimum for the first criterion.

For each game of the bank, the criteria can be configured separately.

If for some player the total RTP of the corresponding game for a certain number of rounds goes for the limits of the criterion for such an interval of rounds, then the tool sends a notification to the specified email addresses.

The disadvantages of this tool are that the RTP can only be discretized into 3 sections. That is, the accuracy may be lower than necessary. Also, the specificity of each game is not considered.

### 1.3.2 AAMS RTP Monitoring

This tool is issued only for AAMS banks. Like Fraud Control, this tool allows to receive notifications in cases where the RTP of a game for a particular player goes beyond certain limits. However, in this tool there is no discretization for several intervals. The allowable maximum value of the RTP is calculated directly for the current value of the rounds using the game SD.

That is, the accuracy of this monitoring is higher. However, the minimum round limit is also set to 10000 to prevent false positives from the alert system.

The algorithm of this tool is as follows:

The statistic is collecting during the game. The statistic includes number of bets, sum of bets, total win. The statistic is grouped by the additional attribute which depends on the particular game (SD).

When the game session is closed all the statistics is summarized into one record which contains the sum of data per day.

Data per day summarized with the total period data once a day.

In case of any issues the customer receives an email with bank name, game name, current rounds/betSum/winSum, current RTP, RTP range. Betsoft Tech Support receives the copy of this notification too.

Tech Support must register this issue and start to identify the root causes. The game must be disabled until the issue is not resolved. After the root causes are clear, the issue should be resolved (i.e. the bugs fixed in the game). Also, during the investigation step some parameters this issue influenced should be calculated. These parameters are the total amount of rounds, bets and wins.

After that the data in the RtpDaily, RtpSummary tables must be corrected. There are investigatedRounds, investigatedBetSum, investigatedWinSum fields where the correction values should be inserted to avoid the influence on the further RTP monitoring process.

In case the correction is not done there will be the further daily triggering of the same issue.

The disadvantages of this implementation:

- At the time of implementation SD did not exist for all games (the list of games is limited).
- The implementation is too resource intensive and therefore cannot be activated for all banks of all systems.
- Monitoring can only be done at 10,000+ rounds.

# Functionality

Based on sections 1.2 and 1.3 it is possible to determine the requirements for the new program. The already existing programs listed in section 1.3 have disadvantages and do not meet the criteria for recognizing the abuse of progress of games.

The new tool should have several features to detect suspicious players:

1. RTP monitoring of the player's gaming activity (as well as the programs described in section 1.3).

2. RTP monitoring of the gaming activity of the entire bank.

3. Compiling a list of bank players playing only one game.

Each functionality must have a set of configuration parameters.

The program must have a notification system for suspicious activity according to the specified configurations and criteria, as well as an emergency game shutdown system when special criteria are met.

## 2.1 RTP Monitoring by the player

The program should monitor the activity of each player and calculate the RTP of each game. Based on the game SD, the program should check for deviations of the player's current RTP from the theoretical maximum RTP for a certain number of rounds of game.

The program should calculate (according to formula 1) the maximum RTP for a given number of rounds of a player's game based on the SD. Unlike the AAMS implementation (section 1.3), now SD is available for most games (0011604 thread in mantis).

Formula 1:

- Upper Limit of RTP for specific number of rounds = RTP by model(provided) + Confidence Factor.
- Confidence Factor = Critical Value (2.58 or 1.96 depending on the required accuracy 99% and 96% respectively) X Standard Error.
- Standard Error = SD(provided) / $\sqrt{RoundsCount}$

If the calculation based on SD is too resource intensive and impossible to implement, the program should use another method. Based on the SD of each game, the intervals of rounds and the corresponding limit of the maximum RTP for these intervals should be calculated. That is, the functionality is similar to the implementation of Fraud Control (section 1.2) but with higher discretization, and also based on the SD of each game. In such a case, the discretization parameter (the number of such intervals) must be configurable. That is, for a specific game, an interval is taken from 10,000 rounds (minimum) to 10,000,000 rounds (maximum for sufficient accuracy), the parameter N (discretization frequency) is selected, after which, based on the SD of this game, intervals of the following form are compiled (for example, the discretization is 10,000 rounds):

1. 10,000-20,000:

- RTP Max 1.98 – Calculated based on formula 1 for the arithmetic average of the number of rounds from the interval (15 000).

2. 20,000 - 30,000:

- RTP Max 1.96

etc.

Monitoring must start at a minimum of 10,000 rounds for a game of player.

If the monitoring detects that the RTP of the player's game is exceeded, then information about the game and the player must send a notification and process this case in accordance with section 2.5.

### 2.2 Bank RTP Monitoring (TBD)

This functionality should use the methods of checking the deviation of the RTP of games based on the SD as for section 2.1, but for the entire bank. This check should be performed only once in a certain period (pre-configured and measured in days).

If the check is configured once a day, then the program should check the deviation of the RTP of each game on the bank, considering the number of rounds and based on the SD of the game every day.

If the current RTP for any case exceeds the calculated one, then the program must send a notification and process this case in accordance with section 2.5.

### 2.3 Checking accounts with one game (TBD)

Since RTP monitoring can only work with 10,000+ played rounds for a game, it is difficult to track accounts that exploit the vulnerability of one game on a small number of rounds. In addition, players often use multi-accounting (as it was in 1.1.2). It was also noticed that in most cases where the vulnerability of the game was used, the player played only this game. This functionality should allow detecting large increases in accounts that play only one game and have an RTP>100.

This functionality must be properly configured. The check should take place every few days (set during configuration).

The program should check how many new accounts have appeared that have played only one game (only for REAL mode) and have an RTP>X% (X – configurable parameter). If during the checking period the number of such accounts for any game exceeded N (configurable parameter), then the program should send a notification (in accordance with section 2.5).

The program should also check players who were on the list of the previous check interval. If there are accounts that have increased RTP and still play only one game, then the program should notify about these players at the current checking period.

### 2.4 Notifications and handling

For functionalities 2.1 - 2.3 there should be a notification system using email. The program should have a list of common email addresses (for all cases of the entire cluster) as well as the ability to specify specific email addresses for each bank.

In the event of an alarm recipients should receive an email of the following form:

- For RTP Monitoring by player.

| | |
|---|---|
| Title | Fraud Control: RTP for player [EXT_ID] |
| The player's RTP has exceeded normal values:<br>[CLUSTER] – bank [BANK];<br>ExtId: [EXT_ID];<br>Game: [GAME_NAME];<br>RTP of player for this game: [CURRENT_RTP];<br>Theoretical RTP: [RTP];<br>GameSessionId: [GAMESESSION_ID];<br>Total rounds for this game: [TOTAL_ROUNDS];<br>Total Bets (EUR): [TOTAL_BETS_IN_EUR];<br>Total Wins (EUR): [TOTAL_WINS_IN_EUR];<br>The game turned off on this bank. (Optional)<br>Link to control panel: [link to the interface where it is possible to confirm the absence of problems and disable repeated notifications for this player] | |

- For RTP Monitoring by bank.

| Title | Fraud Control: RTP for bank [BANK] |
|---|---|
| The RTP of the game for the bank has exceeded the allowable value:<br>[CLUSTER] – bank [BANK];<br>Game: [GAME_NAME];<br>RTP for this game: [CURRENT_RTP];<br>Theoretical RTP: [RTP];<br><br>The game turned off on this bank. (Optional)<br>Link to control panel: [link to the interface where it is possible to confirm the absence of problems and disable repeated notifications for this bank] | |

- For accounts with one game.

| Title | Fraud Control: many new players for [GAME] |
|---|---|
| There are a lot of new players playing [GAME] with RTP>100%:<br>[CLUSTER] – bank [BANK];<br>Game: [GAME_NAME];<br><br>Link to control panel: [link to the interface with all "suspicious" players of the given bank and links to their profile in CM] | |

The program should be able to automatically turn off the game on the bank (optional) in case of an alarm during checks 2.1 and 2.2. For 2.3 this function should not be present since false positives are possible in case of poor configuration.

For checks 2.1 and 2.2 the program should send an incident notification every day if the case has not been marked as investigated. There must be a separate interface for this functionality.

## UI/UX

The program should have interfaces for displaying detected cases, as well as marking them as "investigated" to remove them from monitoring and confirm that there are no problems.

Interfaces can be presented as separate web pages or as CM reports. (TBD)