Fraud Policy and Management Document

Version: GMR 1.0

Prepared By: Easyrewardz

July 15, 2025

Confidentiality & Disclaimer

This document is copy-righted, and all rights are reserved. This document may not, in whole or in part, be copied, photocopied, reproduced, translated, or reduced to any electronic medium or machine-readable form without prior consent, in writing, from an authorized representative of EasyRewardz Software Services Pvt. Ltd. It may not be shared or disclosed to individuals or entities without prior permission from EasyRewardz Software Services Pvt. Ltd.

EasyRewardz is trademark of EasyRewardz Software Services Pvt. Ltd. All other trademarks referenced herein are the property of their respective owners.

Copyright reserved © 2025. EasyRewardz Software Services Pvt. Ltd. All rights reserved.

Contents

1. Outliner Analysis Approach for GMR

An outlier is an observation that lies an abnormal distance from other values in a random sample from a population.

Since the above definition in a way depends on the judgement of the analyst to decide what observations should be considered as abnormal for GMR, the approach note aims to identify what constitutes normal observations and set thresholds using GMR data, beyond which observations can be classified as outliers.

The outlier identification approach developed by EasyRewardz for GMR will identify the outliers using certain parameters as mentioned below.

- EasyRewardz will calculate the parameters (i.e., spends, transactions, point redemptions) for pre-defined time periods 6-12-18 months
- At given time intervals (7, 15, 30 days)
- At customer level recursively.

The objective for the above is to identify data points that do not follow a standard pattern for the data under consideration and are extreme values far away from the central tendency of the GMR data.

Complete data by mobile considering the maximum parameter value.

From the final dataset, ER will publish parameters w.r.t percentile ranging from 0.95 to 0.99.

Values in the highest percentile brackets typically indicate outliers.

2. Current GMR Fraud Rules

Time Period	Criteria for fraud detection
1 Day	Transaction > 5
7 Day	Transaction > 20

Threshold Breach Action = Redemption Block only.

So far, we had limited customer data and a nascent user base. To avoid premature and mis calibrated restrictions, we deliberately kept the fraud detection setup lean — with just two active rules:

- More than 5 transactions in a day
- More than 20 transactions in 7 days

While the fraud management system is capable of supporting **multiple rule combinations** across various parameters (e.g., spend, transaction count, visit frequency) and timeframes (1, 7, 15, and 30 days), enabling all of these at intuitive or arbitrary thresholds — **without data-backed baselines** — would have introduced significant operational and customer experience risks:

- Too many genuine users could be incorrectly flagged and blocked

- Redemption-related complaints and confusion could spike
- Early-stage program trust and adoption could be compromised

We consciously avoided this to prevent **customer friction, dissatisfaction, and reputational risk**.

Now, with ~**1 lakh enrolled customers** and their transactional behaviour available from the past 6 months, we are in a position to run a statistical **outlier analysis**. This will allow us to move from intuitive thresholds to **data-driven, percentile-based fraud detection**, ensuring both **protection** and **genuine user experience continuity**.

The current model was a strategic decision to **prioritize program adoption and trust**, while building a foundation for smarter controls as the ecosystem matured.

3. Benefits of Current GMR Fraud Rules

Features	Details	Benefit to GMR
Current Fraud Rules	- 1-Day: Transactions > 5 - 7-Day: Transactions > 20	Prevents potential abuse from unusually high-frequency transactional activity
Penalty/Action	Redemption is blocked for customers who breach these thresholds	Prevents misuse of loyalty points and financial leakage
Automated Daily Check	System runs a check every day at night for rule violations	Enables proactive fraud detection without manual monitoring
UI Actions Available	1. Mark customer as Fraud 2. Add to Exception/Whitelist 3. Bulk Upload via CSV	Operational flexibility for GMR/Easyrewardz team to manage exceptions and fraud tagging efficiently
Parameters Checked	- Transaction Count	Covers high-frequency behaviour
Time Frames Monitored	- 1 day - 7 days	Ensures multi-temporal monitoring of suspicious activity
User Action Limitation Options	- Stop redemption - Stop points accrual - Or both	Flexible enforcement — lets the business decide severity of action based on fraud profile

4. Benefits of Outlier Analysis based Fraud Rules for GMR

Feature	Definition	Benefit
Outlier Analysis Model	Identifies abnormal behaviours based on GMR data using statistical percentile (0.95–0.99) thresholds	Enables more tailored fraud rules, derived from GMR-specific customer patterns available so far
Customer-Level Recursive Analysis	Parameters like spend, transaction count, and redemptions are calculated recursively at customer level over 6, 12, and 18 months	More accurate identification of outliers based on evolving customer history
Time-Based Parameterization	Analysis done across 7, 15, and 30-day intervals	Captures short-term as well as long-term behavioural anomalies
Segmentation by Mobile Number	Data split by mobile number; max parameter value considered	Ensures individual-level analysis, avoiding aggregate-based errors
One-Timers & Repeaters Classification	(As per system placeholder fields) Segregation planned based on bill count and total spend for fraud detection logic	Enables tiered fraud strategy based on engagement style
Percentile-Based Thresholds	Final dataset will publish 95th–99th percentile brackets for metrics like spend, txns, redemptions	Shifts fraud detection from static rules to dynamic, data-driven thresholds specific to GMR's user base
Metrics Linked to CLTV Components	Frequency × ATV used to drive fraud rule calibration	Ensures differentiation between high-value loyalists and outliers gaming the system
System Rule Combinations	8 combinations across Spend & Transaction for different timeframes (e.g., 1-day spend, 7-day transaction count, etc.)	Ensures coverage of different fraud behaviours without relying on a single threshold

5. Scope

The policies apply to any fraud or suspected fraud. It includes the fraud activities and the methodology to detect the fraud actions of customers basis which customers are marked as Fraud.

6. Purpose

The purpose of this document is to detect the fraud activities based on a set of unusual attributes, including transactions and no. of visits.

When these attributes are detected, System mark the customers as potentially fraud.

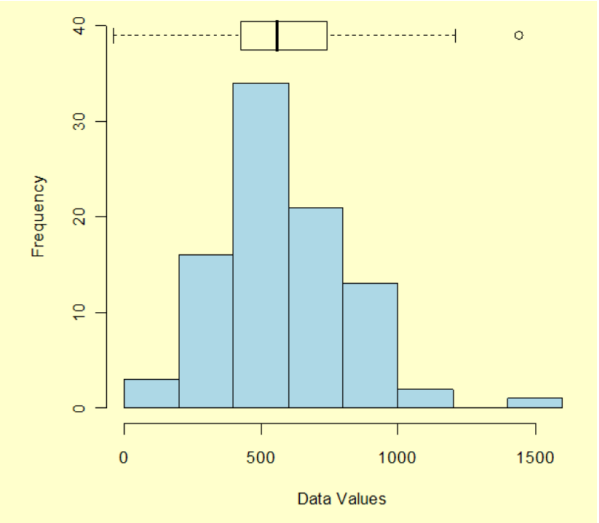
7. Methodology

Below are the methods that helps the system to analyze the customers on the basis of threshold values which is already saved in the system.

7.1. Outlier Analysis

An outlier is an observation that lies an abnormal distance from other values in a random sample from a population.

In a sense, this definition leaves it up to the analyst (or a consensus process) to decide what will be considered abnormal. Before abnormal observations can be singled out, it is necessary to characterize normal observations.



The outlier is identified as the largest value in the data set and appearing as the circle to the right side.

7.2. Outlier Detection

An outlier model has been developed by Easyrewardz to identify the outliers for the above-mentioned rules.

1. We calculate the parameter (i.e., spends, txns) for the following
   - Given time frame (i.e., last 6,12,18 months)
   - At given time intervals (7, 15, 30 days)
   - At customer level recursively.

2. We then split the complete data by mobile considering the maximum parameter value.

3. From the final dataset, we publish parameters w.r.t percentile ranging from 0.95 to 0.99. Patternis highest percentile is observed to decipher the best value for threshold.

7.3. Metrics Calculation

Since Points accrual are decided on basis of Customer Lifetime Value (CLTV), which is function of frequency and ATV. Hence, by studying these features and performing univariate analysis, we can target customers for points accrual as well as fraud detection.

Considering we don't have any historical customer data available and hence we can't share analysis or suggest a spend or visit based fraud policy

One Timers-

1. **Bill count >=**

2. **Total spend >=**

Repeaters-

1. **Frequency >= 20**

2. **Total spend >=**

3. **Total bills**

8. Configuration

The service runs every day 3 AM. It checks if a customer is getting mapped against the fraud rule based on different kind of rules. Transaction value and the count is checked and tracks if some customer has spent more than thethreshold value. Those customers are marked as Probable Fraud customer.

Customer data is analyzed based on the following parameters for different time periods.

1. Spend
2. Transactions

Time Frame Involved:

1. Single Day* (Only for Spend)
2. Weekly
3. Bi-Weekly (15 days)
4. Monthly

The total combinations of rules generated basis of parameters and time frames are 8 which are asfollows:

Time Period	Parameter
1 Day	Spend >=
1 Day	Transaction >=
7 Day	Spend >=
	Transactions >=
15 Day	Spend >=
	Transactions >=
30 Day	Spend >=
	Transactions >=

These rules can be prioritized. E.g.

- 1 day Spend is highlighted over 7 days spend, or
- 7 days Transaction is highlighted over 7 days Spend.O

Once the data points reach to the threshold value a customer is marked as probable fraud customerin our system.

Now, user has three options in the system:

1. **Mark Fraud:** Mark customer as Fraud on UI.
2. **Add to Exception:** If the transaction is genuine then mark as an Exception
3. **Download CSV File:** Extract the data and share it to Easyrewardz team to upload it in bulk tomark the customers as a Fraud.

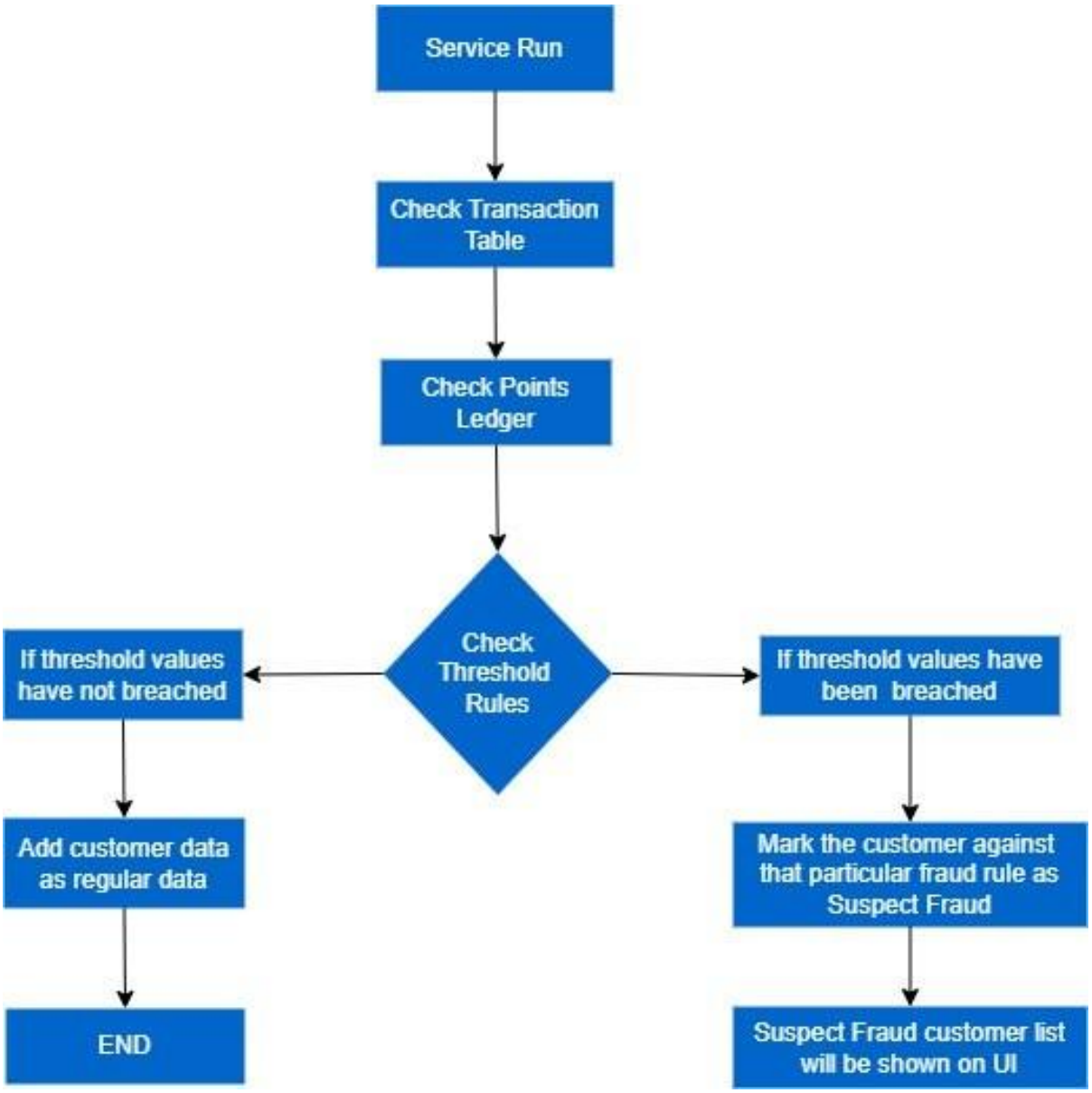
If user has been marked as Fraud, then these rules can be applied for the customers:

1. Stop customer from redeeming the points
2. Stop points accrual for the customer
3. Both 1 and 2

9. Fraud Management

Below are the flowcharts defining the Services run at ER end and customer journey at store:

9.1. ER Service Flow



9.2. Customer journey at store