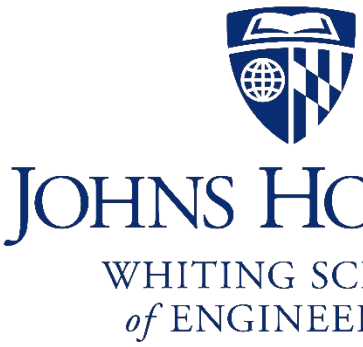


Center for
Leadership Education

Master of Science in Engineering Management (MSEM)

Fall 2024

Fraud Detection Strategy for Shopkick

Project Host

Richard Froggatt

Ido Birger

Team Members

Daniel Ardila

Sharvi Dadhich

Sriaansh Sahu

Chuyang Yu

Table of Contents

1. Executive Summary

Shopkick, a leading rewards-based shopping app, operates in a highly competitive market alongside players like Fetch, Ibotta, Rakuten, and Upside. While Shopkick's unique real-time rewards model offers significant differentiation, it faces critical challenges in fraud prevention, which have resulted in substantial financial losses exceeding $3.5 million in 2024. Fraudulent activities undermine operational efficiency, user trust, and overall platform sustainability.

The primary goals of this project were to analyze Shopkick's current fraud detection system, identify vulnerabilities, and propose actionable solutions to mitigate fraud while maintaining a positive user experience. The project utilized a data-driven approach, leveraging fraud reports, redemption data, user surveys, and stakeholder collaboration to understand the scope of fraudulent behaviors and their financial implications.

Key Findings

- **Fraudulent Activities**: Account creation abuse, promo/receipt fraud, and redemption manipulation are the leading contributors to losses.
- **Patterns in Fraud**: Fraudulent users exhibit predictable and automated behaviors, such as immediate transactions after account creation, leveraging promo codes repeatedly, and uploading manipulated receipts.
- **Verification Gaps**: Absence of mandatory phone/email verification and tiered payout checks are key vulnerabilities.
- **Financial Impact**: Receipt fraud alone resulted in $1.76 million in losses, while promo code abuse contributed to $336,102 in losses in 2024.

Recommendations

To address these challenges, the team developed and prioritized the following solutions:

1. **Account Creation Modification**
    a. Introduce mandatory phone and email verification within 24 hours of account creation.
    b. **Impact**: 75% reduction in fraudulent account creation.
2. **Bracket Payout Verification**
    a. Implement tiered verification thresholds for redemption amounts, requiring stricter checks for higher payouts.
    b. **Impact**: Prevent a $71,000 loss annually while retaining 99% of legitimate users.

3. **Workflow Redesign**
    a. Establish earning limits across activities like barcode scanning and receipt uploads, with automated flagging for suspicious behavior.
    b. **Impact**: 26% reduction in fraudulent users earning kicks.
4. **Promo Code Prediction**
    a. Use predictive algorithms to detect and limit promo code abuse, focusing on high-risk codes.
    b. **Impact**: 49% reduction in fraudulent promo code redemption when tested on FSF over 6 months.
5. **First Redemption Limit**
    a. Restrict initial redemptions based on account age and activity patterns.
    b. **Impact**: For every $1,251 redeemed, $1 of fraud is prevented.

Anticipated Outcomes

The implementation of these recommendations is expected to:

- **Reduce Financial Losses**: Save millions annually by minimizing fraud.
- **Enhance User Trust**: Strengthen security and deliver a better user experience.
- **Optimize Operations**: Automate fraud detection processes, reducing manual intervention.
- **Reinforce Market Position**: Improve Shopkick's appeal to both users and brand partners by demonstrating robust fraud prevention measures.

2. Introduction/Background

Shopkick operates within a highly competitive shopping rewards market, with primary competitors Fetch and Ibotta, alongside industry players like Rakuten and Upside. Shopkick differentiates itself through high consumer engagement across the entire purchasing journey, leveraging a unique pay-for-performance model that maximizes ROI for brands. The platform emphasizes immediate rewards—known as "kicks"—for activities such as in-store walk-ins, product scans, and purchases, creating a dynamic, hands-on marketing approach. While this strategy overlaps with Fetch and Ibotta, these two competitors focus primarily on post-purchase activities like receipt uploads and cashback offers.

Among Shopkick's and its direct competitors, Fetch and Ibotta, business models are similar. Despite its smaller active user base (see the table below) compared to Fetch and Ibotta, Shopkick offers a unique value proposition of real-time rewards for pre-purchase engagement. All three partner with retailers and brands that pay to run campaigns for their products. While Fetch aims to build up its data analysis abilities to better target consumers and provide brands with market insights – Fetch and Ibotta already process this data are large scales.

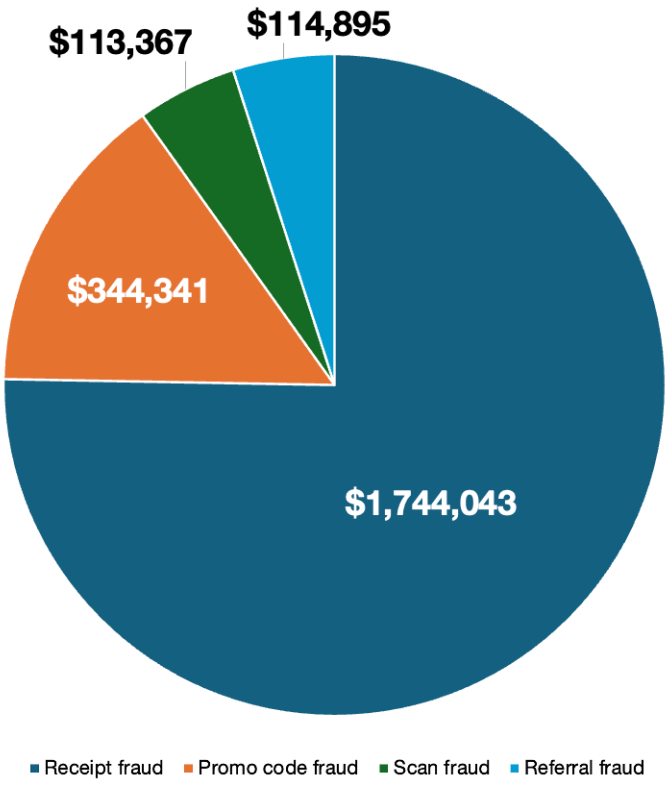


Figure 1. 2024 YTD Fraud at Shopkick broken down by type

The three platforms all see some level of fraud inherent to the rewards-based nature of the apps as fraudsters target the low, or even medium-effort required to circumvent existing fraud measures. As Shopkick loses millions in fraud, it faces a more diverse range of fraud than its strictly post-purchase rewards competitors. These measures to stem this fraud can be contextualized by market standards in fraud prevention organization, account creation, and payout structure.

2.1 Fraud Prevention Organization

Shopkick's diverse range of methods for earning 'kicks' makes its fraud problem more multifaceted than its competitors as it faces not only receipt fraud but fraud from fake barcode scans, falsified walk-ins, and promo code abuse among others.

	Shopkick	**Ibotta**	**Fetch**
Methods for Earning Kicks/Points/ Money	Walk-ins, Product scans, Purchases, Videos, Referrals, Promo Codes	Offers on purchased items, Brand bonuses, Referrals	Receipts (e and paper), Games, Offers, Referrals, Points boosts
User Base	400,000 monthly users	11.9 million users in Q2 2024. [1]	17 million monthly users as of 2022.[2]
Employees	50-75 employees	~ 988 employees [3]	~ 734 employees

While Shopkick is the smallest of these 3 market competitors by market share (see *Figure 1* in the appendix), user base, and employee numbers. It is the only rewards app that lacks a dedicated fraud team. As seen in Appendix *Figure 2,* Ibotta has a dedicated fraud team of at least 14 employees based out of Denver. In *Figure* 3, Fetch's large 44-person team based in the U.S. and Mexico span data analyist and fraud specialists. The size of these teams, coupled with their choice of fraud software w has allowed them to process billions of transactions and give out hundreds of millions of rewards without fraud limiting scaling potential. [4][5]

2.2 Account Creation

The opportunity for fraud begins when an account is created. Over the past 4 years, Shopkick has shifted its requirements and developed more robust ways of flagging individuals with suspicious emails, versions of iOS, device names, IP addresses, etc…; however, many malicious users are able to create accounts and commit fraud on a daily basis. This difficulty in identifying fraudsters versus honest users makes it hard to track campaign success and accurately understand Shopkick growth among other costs in combatting fraud.

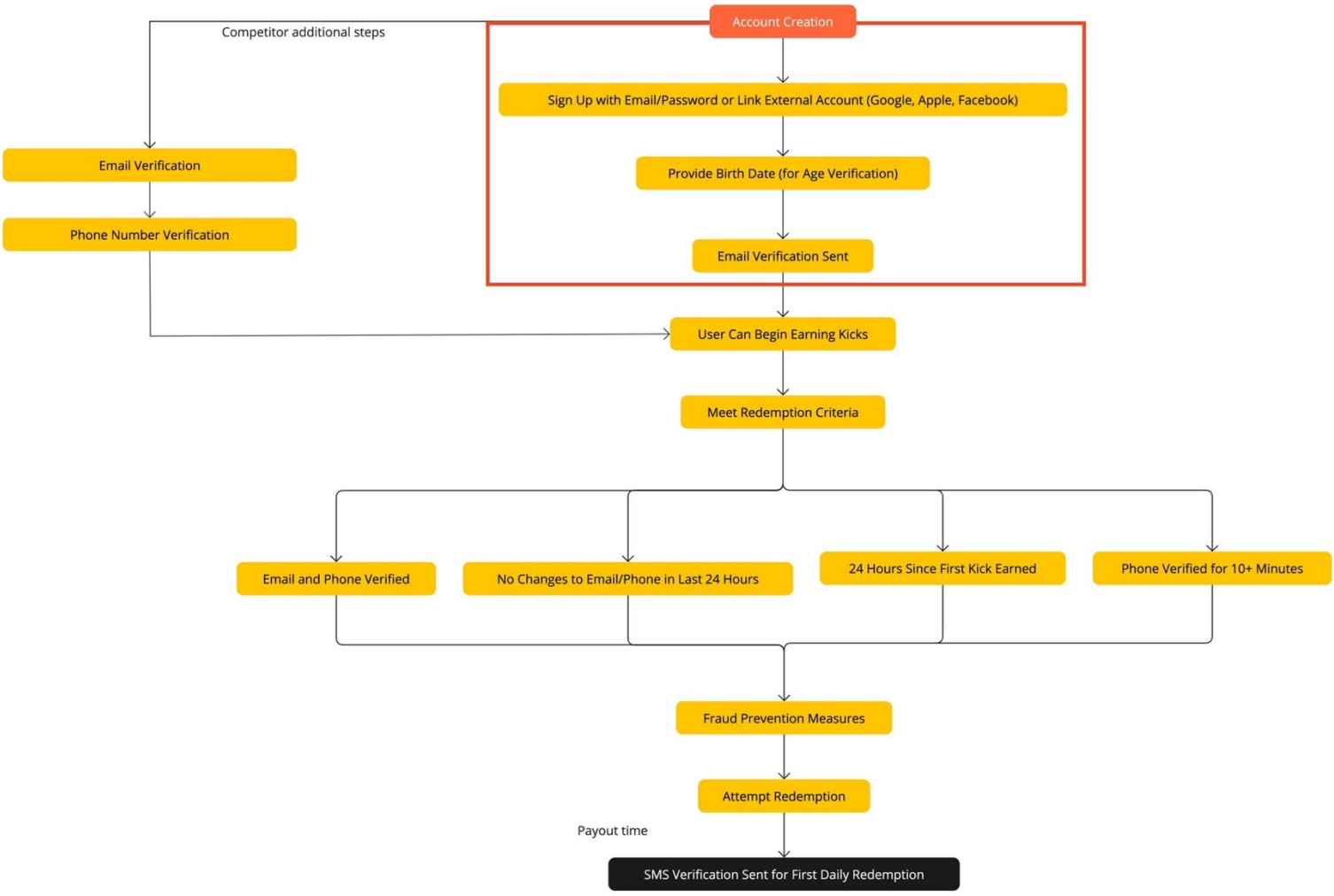


Figure 2. Shows the account creation process for Shopkick as well as the added steps competitor's feature

The flow chart above identifies the current path that users follow when creating an account. To the left of the diagram are some additional steps that competitors require such as phone number verification at account creation (and redemption). We explored this gap between Shopkick and its competitors to analyze if Shopkick could implement this measure and found that it would be beneficial to require phone number verification at account creation. This finding, and its impact, are detailed in the recommendations section.

2.3 Payout Structure

Crucial to the understanding of fraud is the payout structure for Shopkick and its competitors. These variables, included in the table below, include the dollar amount required to redeem (for the first time ever and each subsequent redemption), whether or not bank account linking is offered, and how long it takes for users to receive gift cards or 'cashback.'

	Shopkick	Ibotta	Fetch
$ to redeem	$2	$10 first time, $3, $5 available after	$20
Phone verification at account creation	No	Yes	No
Bank Account	No	No	Yes
Time to receive gift card	Most are immediately available (can take a few hours depending on shopper traffic)	3-day delay for "account security"	Immediately for PayPal/gift card 1-3 days for bank

It is important to notice that Shopkick has a much lower value for the amount required to redeem – this has informed our recommendation to eliminate the $2 gift card and require a $10 gift card for the user's first redemption. Additionally, it is important to note the delay that Fetch employs between giving out gift cards – a feature that allows its teams to verify redemptions. While Shopkick's instant gift card awarding is a draw to users, the tradeoff between speed and security was additionally considered in our analysis.

2.4 Tool Benchmarking

While dedicated fraud teams create key advantages for Ibotta and Fetch, the 2 competitors also use different software for fraud detection. The comparison of their key features is shown in *Appendix 6*.

Shopkick leverages Sift for fraud detection, a software that relies heavily on AI intervention and offers data monitoring, though it requires customization during setup. A primary complaint from the Shopkick team is the lack of truly real-time data and the disjoint dashboards that are created by the analytics team since they are not able to make wholistic and specific data requests from Sift directly

Fetch relies on Kount, known for its advanced fraud detection using device fingerprinting and behavioral analytics. Though some users face integration challenges, the solution has greatly reduced Fetch's need for manual intervention – dropping this number to only about 2% of transactions being manually reviewed. [6]

Ibotta utilizes Imply, which excels in scalability and advanced analytics with Apache Druid, enabling real-time anomaly detection and effective monitoring of high-volume transactions. Imply's integration with the data river structure seems to solve the real-time data problem that plagues Sift. [7]

3. Methodology

3.1 Sift Investigation

Sift is the primary platform used by the Shopkick team for fraud detection and prevention. The platform scores user behaviors based on various parameters, with higher scores indicating a greater likelihood of being a fraudster.

By obtaining read access to the Sift system, we gained a clearer understanding of users' kick-earning actions. This access enabled us to identify distinct characteristics of different fraud users and distinguish patterns between fraudulent and legitimate users.

3.2 Fraud Data Analysis

We obtained extensive data from Shopkick's multiple teams and data analyst Chris Gee, including, but not limited to, the 2024 fraud report, the number of banned users and the amount they redeemed, user churn rates, randomly sampled email addresses of 1,000 users, and redemption amounts across various kick-earning actions.

This data significantly helps us to establish user redemption brackets, analyze the lifetime patterns of promo codes, and identify characteristics of suspicious users.

3.3 Multi-team Interviews

During the 6-week project, we held weekly online meetings with different Shopkick teams and roles. In these meetings, we discussed our weekly progress, raised questions, and addressed issues.

	Engineering	Operations	Marketing
Team Function	Development and maintenance of the application including adding functionalities of the application and workflow creation.	Detect and prevent fraud by monitoring and blocking fraudulent activities (user accounts, receipts upload, etc.).	Retain users through improving promo codes and referral programs while avoiding potential fraud.

3.4 Facebook Group Survey

Balancing fraud prevention and user experience has always been our goal. To better evaluate the impact of our recommendations on user experience, we collaborated with the marketing team to design a survey for Shopkick's fan group on Facebook. The survey included questions about users' preferences when redeeming gift cards, their willingness to accept additional verification or link their bank accounts, and suggestions for improvements. Within a week, the survey received 70 responses.

4. Analysis

4.1 Overview

To further understand the challenges Shopkick is facing, we organize the user journey into 3 sequential stages: account creation, kick earning and redemption. Each stage highlights potential fraudulent activities having an impact on both Shopkick and legitimate users.

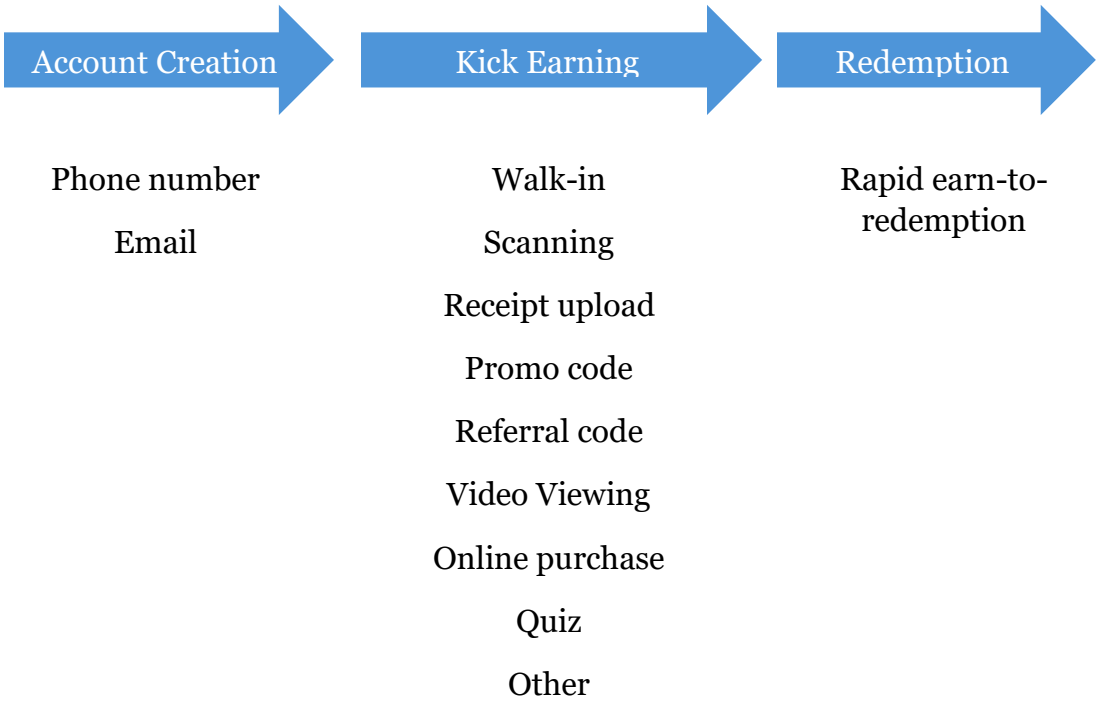


Figure 3. Breakdown of fraud activities

This structure provides a clear picture of where and when the fraudulent activities occur, helping in targeted fraud detection and prevention strategy.

4.2 Fraud Types

By calculating and analyzing data for each type of fraud, we can assume their frequency and cost, as shown in the table below.

Fraud Types	Frequency/100 users	Cost/$
Phone number	25	627,720.97
Email	22	525,089.79
Walk-in	4	18,201
Scanning	2	113,481
Receipt upload	2	1,761,931
Promo code	2	336,102
Referral code	2	116,451

The following sections provide a detailed analysis.

4.2.1 Phone Number

Fraudulent activities related to phone numbers primarily exploit Shopkick's lack of phone number verification during account creation and a loophole in Sift's logic: as long as an account exists for 24 hours, it can redeem kicks for gift cards or cash.

The specific fraudulent activities can be categorized into two types:

- Verifying the phone number only at the time of redeeming
- Purchase disposable numbers for each redemption

Frequency: 25.3/100

Out of 52 fraud users randomly sampled, 29 cases verified their phone numbers 3 days after account registration. For both legitimate users and fraudsters, phone number frauds have an occurrence frequency of 25.3%.

Cost: $627,720.97

There is no direct data source, but according to the fraud user report, Shopkick granted 596,692,939 kicks to banned users from January to October this year. Based on the fraud frequency and the conversion rate of 250 kicks = $ 1, it can be estimated that this type of fraud caused a loss of $ 627,720.97.

User characteristics: frequently changing phone numbers

4.2.2 Email

We sampled 1,000 users and the email addresses they used to create their accounts and found that the majority were Gmail, Outlook, and Hotmail addresses. Among them, the probability of fraud for Gmail accounts was 38.6%, while it was 87.5% for Outlook and 79.5% for Hotmail. Therefore, we focused on the latter two (which aligns with the fact that Outlook and Hotmail accounts do not require phone number verification during registration).

Frequency: 22/100

Among these 1,000 users, a total of 220 users with Hotmail or Outlook accounts were flagged as fraud by Sift.

Cost: $525,089.79

Similar to the phone number fraud situation, using the occurrence frequency and conversion rules, we can estimate the monetary loss associated with suspicious email accounts.

User characteristics: email usernames are randomly generated, email accounts have a relatively short age

4.2.3 Walk-in

Shopkick allows users to earn 10 kicks by walking into a physical store. However, during this process, some users manipulate their location to fraudulently claim kicks. The biggest challenge for Shopkick in this type of fraud is the inability to gain information on whether customers actually entered the store.

Frequency: 4/100

Using data from October 2024 as an example, a total of 678,821 users earned kicks on Shopkick, among whom 29,811 users were flagged as fraud by Sift and had their accounts frozen due to walk-in activities.

Cost: $18,201

From Jan to Oct 2024, users banned for walk-in type fraud collectively earned 4,550,265 kicks. Based on the conversion rate, the monetary loss caused by this behavior can be calculated.

User characteristics: use VPN/jailbroken, show suspicious IP organizations

4.2.4 Scanning

Users can earn 10 to 25 kicks by scanning the barcodes of specified products. However, the number of scans is limited; for example, the same product can only be scanned once per week, and the total number of scans per week cannot exceed 20. After scanning, a brand-sponsored survey may pop up randomly.

Scanning-type fraud can be mainly categorized into two types:

- Barcode scans
- Shelf scans

Some users exploit this by scanning pre-prepared images or screenshots to earn kicks.

Frequency: 2/100

Using data from October 2024 as an example, a total of 678,821 users earned kicks on Shopkick, among whom 6,477 users were flagged as fraud by Sift and had their accounts frozen due to scan activities.

Cost: $113,481

From Jan to Oct 2024, users banned for scan-type fraud collectively earned 28,370,281 kicks. Based on the conversion rate, the monetary loss caused by this behavior can be calculated.

User characteristics: short scanning intervals, use VPN/jailbroken

4.2.5 Receipt Upload

Users can earn corresponding kicks by uploading receipts with specified products. According to the data, some users have redeemed a total of $1,012 from receipt uploads, also making receipt-type fraud the biggest challenge Shopkick currently faces. The fraudulent activities may include the following types:

- Uploading blurry images
- Printing multiple receipts on their own
- Re-uploading the same receipt multiple times
- Altering or forging original receipts

Frequency: 2/100

Using data from September 2024 as an example, a total of 685,838 users earned kicks on Shopkick, among whom 9,792 users were flagged as fraud by Sift and had their accounts frozen due to receipt uploading activities.

Cost: $1,761,931

From Jan to Oct 2024, users banned for receipt-type fraud collectively earned 440,482,701 kicks. Based on the conversion rate, the monetary loss caused by this behavior can be calculated.

User characteristics: all Shopkick-specific/high-kick items on the receipt, mass uploads in a short time

4.2.6 Promo Code

Shopkick collaborates with platforms or influencers to release promo code links, allowing users to earn $5 in cash through these links. The main types of promo codes are as follows:

- Affiliate (e.g. Facebook)
- Influencer (e.g. Instagram, YouTube)
- Paid (e.g. Facebook ads, Apple search ads)
- Organic (Shopkick)

Currently, these promo codes have no limits on usage or expiration, leading to redemption spikes even four years later (e.g., FSF, LOGAN, etc.). Additionally, the wide variety of promo codes enables users to abuse them while leading to other types of fraud

(online purchases). The automatic and fast nature of promo codes also makes fraud detection challenging.

Frequency: 2/100

Using data from September 2024 as an example, a total of 685,838 users earned kicks on Shopkick, among whom 11,503 users were flagged as fraud by Sift and had their accounts frozen due to promo code activities.

Cost: $336,102

From Jan to Oct 2024, users banned for promo code fraud collectively earned 84,022,574 kicks. Based on the conversion rate, the monetary loss caused by this behavior can be calculated.

User characteristics: new users, count for tasks other than promo codes is almost 0

4.2.7 Referral Code

This is a type of promo code where each user has a unique referral code to earn kicks by inviting new users, typically earning $1–2. While there are usage restrictions (100), some users misuse this by sharing referral codes among multiple fake accounts to earn kicks.

Frequency: 2/100

Using data from September 2024 as an example, a total of 685,838 users earned kicks on Shopkick, among whom 10,183 users were flagged as fraud by Sift and had their accounts frozen due to invitation activities.

Cost: $116,451

From Jan to Oct 2024, users banned for invitation fraud collectively earned 29,112,650 kicks. Based on the conversion rate, the monetary loss caused by this behavior can be calculated.

User characteristics: new users with suspicious email

4.2.8 Other

Other types of fraud include video viewing, online purchases, and quizzes. Based on data from January to October 2024, the monetary losses from these types account for only 1% of all fraud-related losses, which shows a relatively low risk.

Some users complete a large number of kick-earning actions in a short period after account registration and redeem kicks in batches. Since certain kick-earning actions are system-automated and kicks are granted instantly, the system is unable to promptly detect such fraudulent activities.

4.3 Overall Impact

The occurrence frequency of fraud to some extent reflects the operational difficulty level of the kick-earning action: the higher the frequency, the simpler the process. It also indicates weaker prevention by Shopkick for such actions, which can serve as a focus for future improvements.

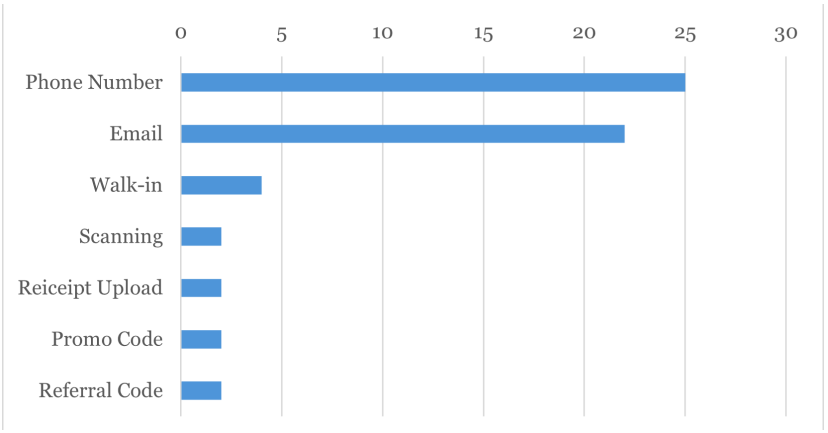


Figure 4 Frequency of Each Fraudulent Activity

The proportion of financial losses from various types of fraud is a key indicator for prioritization. Fraud with the highest financial loss becomes the primary target for risk management. Additionally, the value of losses provides support for allocating resources to following fraud prevention.

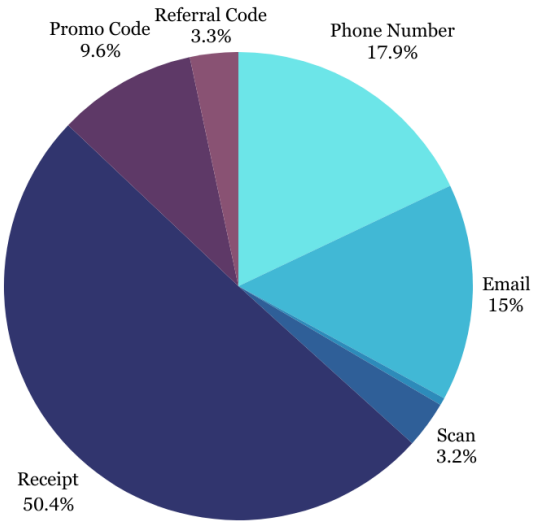


Figure 5 Financial Loss of Each Fraudulent Activity

4.4 Recommendation-driven Analysis

4.4.1 Email and Phone Number Verification

A dataset comprising 52 fraudulent user accounts was utilized. The dataset included fields such as ID, email, Sift score, account creation date, and mobile phone verification date. To ensure unbiased results, the data points were selected randomly. The methodology involved computing the time difference between the account creation date and the mobile phone verification date for each user. These differences were then averaged to derive an overall metric.

The analysis revealed that the average time difference between account creation and phone number validation was 6 days, with an average Sift score of 93. This indicates that users taking more than 6 days to validate their phone number after account creation are likely to exhibit fraudulent behavior. Based on these findings, it is recommended that the time difference be reduced to less than 1 day. Furthermore, phone number validation, along with email verification, should be integrated into the account creation workflow to mitigate fraud risks.

4.4.2 Tiered Verification for Redemption

Identify the redemption range

Analyze the data about cumulative redemption amounts for users flagged as fraud by Sift, primarily concentrated in $2-50

$	#	Total $
2-50	122	2,665
51-100	38	2,807
101-500	75	16,798
501-1000	15	10,273
1001-10030	11	38,455

By further breaking down the $2-50 range, we can set up tiered verification thresholds

$	#	Total $
2-10	52	420
11-20	17	305
21-30	25	659
31-40	5	195
41-50	23	1,086

The table shows that most users count in [2, 10], [21, 30], [41,50], which can help us Set up levels for verification accordingly.

To make sure this recommendation is feasible, we can conduct a cost-benefit analysis.

We can get from KEU and churn data that from Jan to Oct 2024, the average number of new users churned is 16599, that of existing users churned is 64552, and the total amount of KEUs is 280449. We can estimate after implementing stricter verification, we can avoid a $70,998 loss while keeping 99% legitimate users (based on a Facebook group survey).

4.4.3 User Earning Monitoring

For each type of fraudulent activity, including walk-ins, barcode scanning, receipt scanning and uploads, promo code usage, and referrals, data were collected on the total number of fraudulent users involved and the corresponding monetary impact caused by each activity. Additionally, the monetary impact per user for each fraudulent activity was calculated to provide a detailed understanding of the financial repercussions.

During the analysis it was found that per-user earnings vary across different activities: **walk-ins** generate **$0.60 per user**, **product barcode scanning** earns **$2.00 per user**, and **product receipt scanning** provides the highest earnings at **$49.00 per user**. **Promo code usage** yields **$5.00 per user**, while **referral code usage** results in **$3.00 per user**.

To prevent fraudulent activities, if a user exceeds the predefined limit across activities such as walk-ins, product barcode scanning, product receipt scanning, promo code usage, or referral code usage, their account can be temporarily frozen. Alternatively, restrictions can be imposed to make earning rewards less incentivizing, thereby reducing the potential for misuse.

4.4.4 Account Age and 1st Transaction Age:

For this section, two distinct datasets were utilized, both containing common parameters such as the account age of users and the age at their first transaction. The datasets comprised 688 data points from non-fraudulent users and 992 data points from fraudulent users. To derive insights into user behavior, linear regression analysis and t-test: Paired Two Sample for Means were performed on these datasets, and the results were compared.

Insights from linear regression analysis are shown as follows:

Behavioral Insights

Fraudulent Users:

Predictable Behavior: Transactions occur almost immediately after account creation, with minimal variation (tight linear relationship).

Fast Exploitation: Fraudulent accounts typically transact within a day, leaving little time for detection before they act.

Homogeneous Activity: The low residuals suggest fraudulent users act in a highly consistent and structured manner, likely reflecting automated or scripted actions.

Non-Fraudulent Users:

Natural Delays: The negative intercept (-79.35) indicates a lag before non-fraudulent users make their first transactions, potentially reflecting onboarding or user engagement cycles.

Diverse Patterns: A higher standard error (296.96) and lower R2R^2R2 show a wider spread in user behavior. Non-fraudulent users are less predictable and include various transaction timings.

Gradual Engagement: The steeper slope (1.7449) indicates a slower build-up of transaction activity, contrasting the immediate behavior of fraudulent users.

Key Differences Between Fraudulent and Non-Fraudulent Users

Timing of Transactions

Fraudulent users act almost immediately (average delay ≈ 0.66 days).

Non-fraudulent users display a natural lag and require engagement over time (negative intercept suggests longer wait times).

Consistency

Fraudulent users are tightly clustered around their transactional patterns (low residual error, R2R^2R2 ≈ 1).

Non-fraudulent users exhibit variability, indicating diverse user journeys.

Automation vs. Human Behavior

Fraudulent users' consistent and immediate actions likely indicate automated or semi-automated fraud.

Non-fraudulent users reflect more organic, human-like behavior with variability in transaction timings.

Timing Patterns

The distribution of transaction delays for fraudulent users is tightly clustered around near-zero delays (immediate transactions).

Non-fraudulent users exhibit a broader range of transaction delays, reflecting more variability and natural engagement times.

Residual Analysis

Fraudulent users' residuals (observed vs. predicted) show minimal deviations, reinforcing their predictable behavior.

Non-fraudulent users have larger residuals, aligning with their diverse and unpredictable transaction patterns.

Cluster Analysis

Clustering reveals distinct groups:

Fraudulent users form a highly dense cluster with low transaction delays and shorter account ages.

Non-fraudulent users appear in multiple clusters, reflecting varied behaviors.

Transaction Delay Outliers

Outliers in fraudulent users represent attempts to mimic legitimate behavior by delaying transactions.

Outliers in non-fraudulent users reflect users with very delayed initial transactions or unusual activity patterns.

Activity Patterns Beyond Timing

For fraudulent users, additional behavioral metrics (if available, such as transaction frequency or values) could reveal consistent, high-frequency activities.

Non-fraudulent users' behavior metrics would likely show irregular but human-like patterns.

Insights from t-test: Paired Two Sample for Means analysis,

Drastic Difference in Account Age

Fraudulent Users: Accounts are very new (mean account age = ~9 days), indicating most fraudulent activities occur shortly after account creation.

Good Users: Accounts are significantly older (mean account age = ~508 days), reflecting long-standing legitimate activity.

Time to First Transaction

Fraudulent Users: First transactions occur almost immediately after account creation (mean = ~8.6 days).

Good Users: The average time to the first transaction is much longer (mean = ~336.7 days), indicating natural engagement over time.

Variance

Fraudulent Users: The variance in both account age and time to first transaction is very low, reflecting uniform, predictable behavior among fraudulent accounts.

Good Users: Variance is much higher for account age and first transaction time, reflecting diverse and natural behavior among legitimate users.

Correlation

Fraudulent Users: Near-perfect correlation (0.99987) between account age and first transaction timing. This suggests highly automated or systematic behavior.

Good Users: Strong correlation (0.83862) but less perfect, indicating legitimate users' behaviors are not as rigidly tied to account age.

Statistical Significance

For both fraudulent and good users, the t-test shows a statistically significant difference between account age and transaction time, but the nature of the differences is vastly different: for fraudulent users, it can be a minimal, consistent difference, while for good users, it can be a large, varied difference.

Based on the insights from the linear regression and t-test analyses, it is recommended that both the account age and the time to the first transaction be at least 1 day. If either is less than 1 day, there is a significantly higher likelihood that the user exhibits fraudulent behavior.

4.4.5 Verify if the accounts are operated by Humans or not

For this section, two distinct datasets were utilized, both containing common parameters such as the account age of users and the age at their first transaction. The datasets comprised 688 data points from non-fraudulent users and 992 data points from fraudulent users. To derive insights into user legitimacy in terms of whether the user is human or not, linear regression analysis and t-test: Paired Two Sample for Means were performed on these datasets, and the results were compared. Furthermore, the correlation between the account age of users and the age at their first transaction was compared.

4.4.6 Increase the limit for first redemption

Based on our experience using Fetch and Ibotta, we found that the minimum amount for a user's first redemption is $10 or $20, while Shopkick's is relatively lower at $2. From a random sample of 1,000 users' redemption data, most users chose to redeem $25 for the first time. However, for the $2 tier, approximately 10% of users were flagged as fraud, the highest among all redemption amounts, as shown in the figure. Based on these findings, we propose raising the minimum redemption limit for the first transaction to $10.

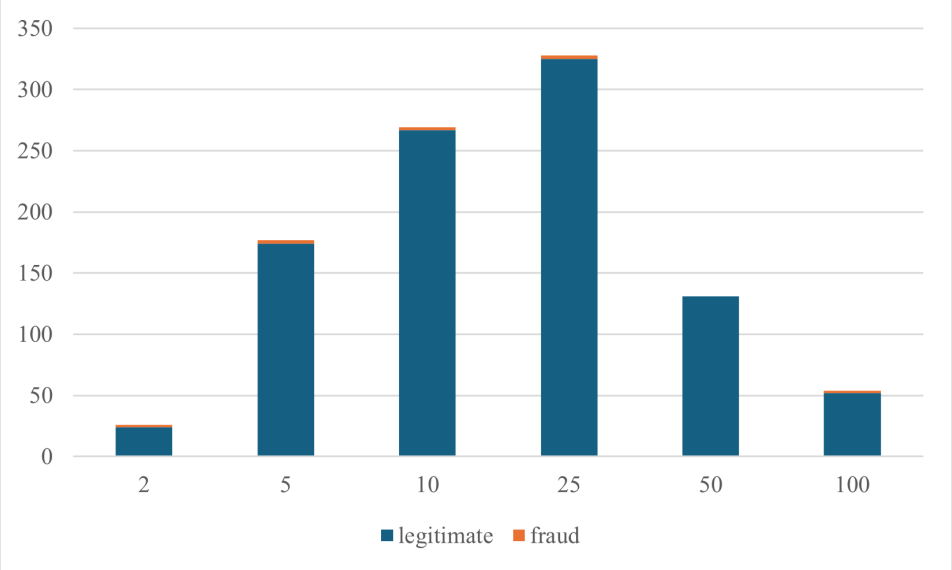


Figure 6 Distribution of the First Redemption Amount within Random 1000 Users

To avoid negatively impacting user experience, we collaborated with the marketing team to conduct a survey in our Facebook fan group about users' redemption preferences. By the end of the survey, we received over 30 comments in total.

The results showed that more than half of the users chose $25 for their first redemption, as shown in *Figure 7*, which is a positive indication.

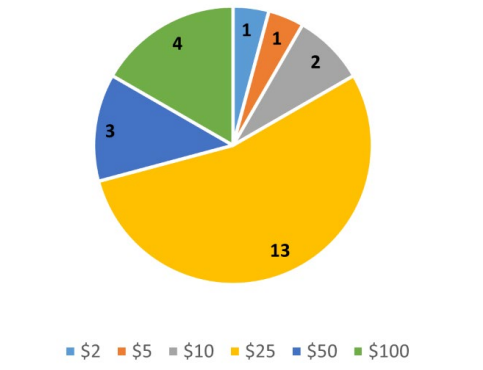


Figure 7 Distribution of the First Redemption Amount within Facebook Fan Group

5. Recommendations

5.1 Email and Phone Verification

Adjustments to the Sift workflow can be implemented to monitor the time elapsed between account creation and the completion of both email and phone verification. If this time difference exceeds 1 day, there is a high likelihood that the user is engaging in fraudulent behavior.

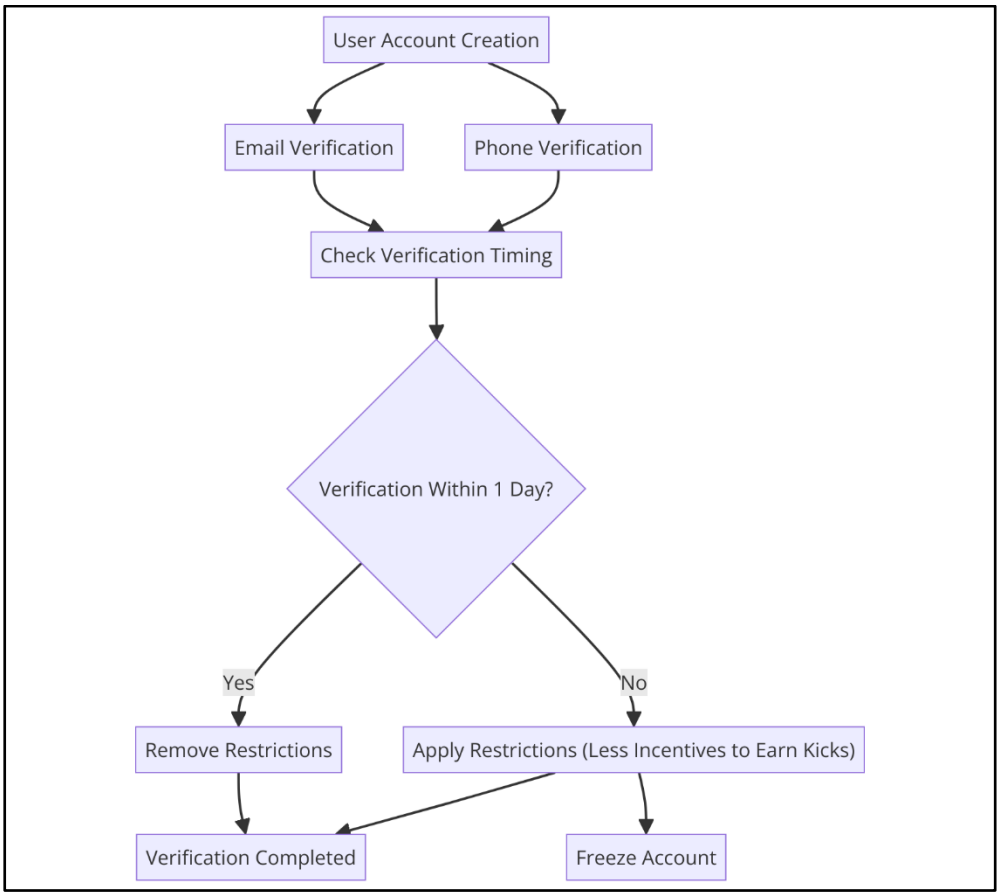


Figure 8 Redesigned Workflow for Account Creation Process

Implementation Timeline:

Time to implement: 1-2 Weeks

This recommendation requires adjustments to existing workflows in Sift, which is straightforward to implement. The key is setting up monitoring for elapsed time and defining thresholds for flagging suspicious accounts. Testing and deployment should not take more than a couple of weeks.

5.2 Tiered verification

Use these brackets as thresholds for different verification levels

$2-25: basic verification-phone number

$50: dual verification- reverify the same phone number/email

$100: government ID

$500: dual verification-the same phone number with government ID

Time to implement: 3-5 weeks

The actual time depends on the complexity of each tier. To have a smoother implementation, Shopkick needs to change its verification workflow and integrate the new thresholds into the app, also inform users about the adjustments. Since stricter verification may increase the difficulty and time required to redeem, continuous adjustments based on feedback are necessary.

5.3 User Earning Monitoring

Adjustments to the Sift workflow can be introduced to address cases where a user exceeds the predefined monthly limit for activities such as walk-ins, product barcode scanning, product receipt scanning, promo code usage, or referral code usage. In such instances, the user's account can be temporarily frozen, or restrictions can be implemented to reduce the incentive for earning rewards, thereby minimizing the risk of misuse.

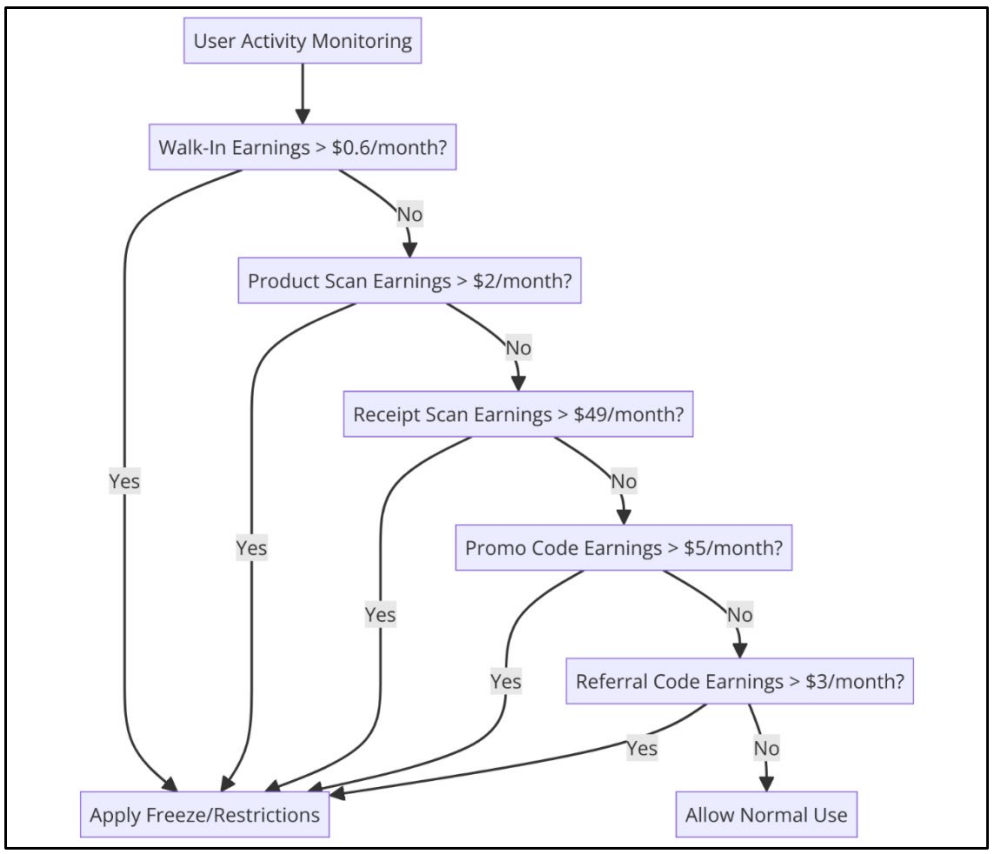


Figure 9 Redesigned Workflow for Sift Fraud Detection

Implementation Timeline:

Time to implement: 3-4 Weeks

Monitoring earning thresholds requires setting up specific parameters for each activity and integrating with the Sift workflow. Additional steps include updating user policies, backend rule configurations, and system testing to ensure smooth functionality without disrupting genuine user activities.

5.4 Account Age and 1st Transaction Age

Adjustments to the Sift workflow can be implemented to flag cases where a user's account age and time to their first transaction are both less than 1 day, as this strongly indicates a high likelihood of fraudulent behavior.

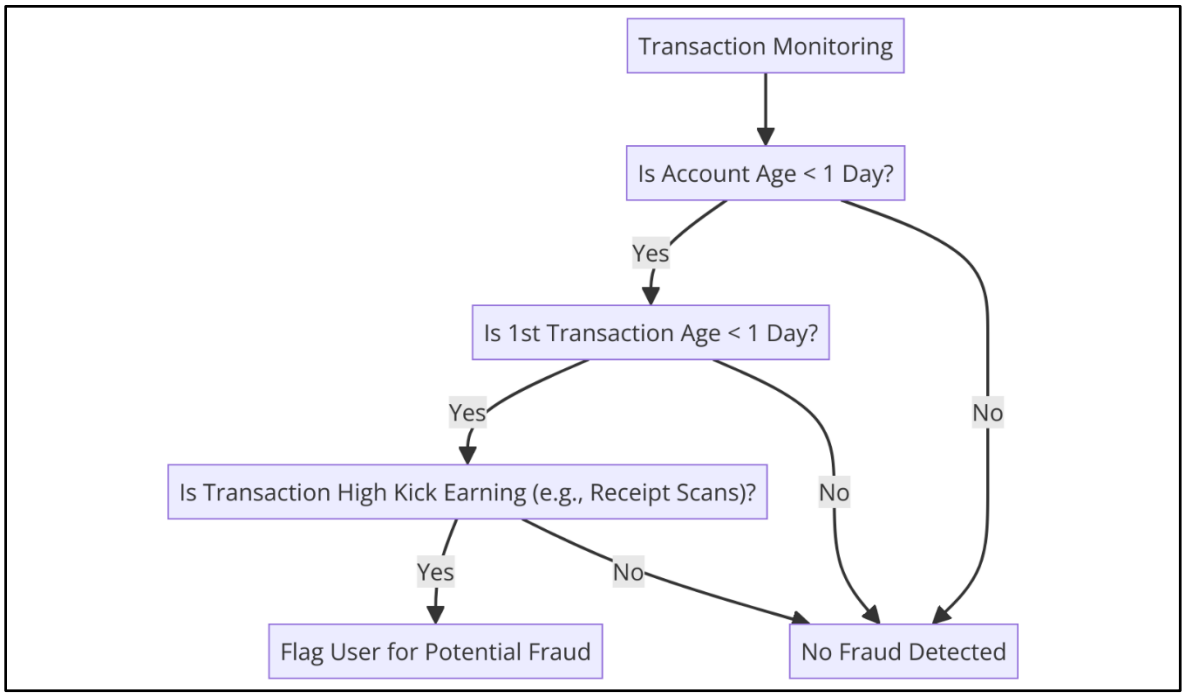


Figure 10 Redesigned Workflow for Sift Fraud Detection Related to Phone Number Verification

Time to implement: 2-3 Weeks

Implementing this recommendation involves adding a simple flagging mechanism based on account creation and transaction timestamps. It's a lightweight adjustment that primarily requires testing to ensure it doesn't generate false positives.

5.5 Verify if the accounts are operated by Humans or not

Adjustments to the Sift workflow can include implementing CAPTCHA verification to distinguish between human users and computer-operated bots.

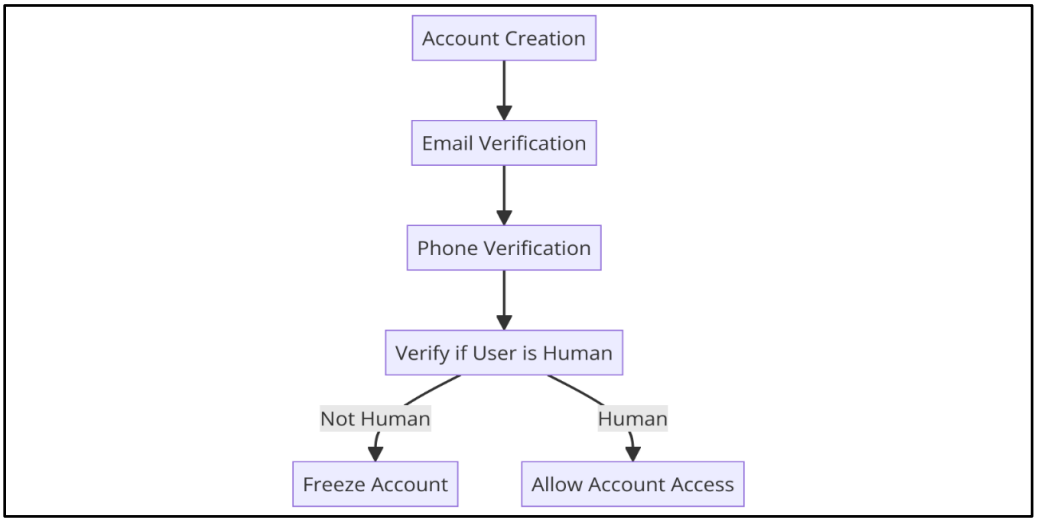


Figure 11 Redesigned Workflow for CAPTCHA Verification

Time to implement: 1-2 Weeks

CAPTCHA implementation is relatively straightforward, but it must be carefully designed to ensure it doesn't deter genuine users. Testing across multiple platforms (web, mobile) and ensuring accessibility compliance will take additional time.

5.6 Increase the limit for the first redemption

Based on the comments from the Facebook group survey and user first-time redemption data from a larger sample size, we propose that Shopkick can consider raising the minimum amount of user first redemption to $10.

Time to implement: 1-2 weeks

This change is relatively easy to implement. The 1-2 weeks are needed to adjust the parameters, update the user interface, and inform users about the updated policy. This time also allows Shopkick to test, which can ensure a smooth implementation and optimize user experience.

6. Conclusion

Fraud prevention is critical to the success and sustainability of Shopkick's business model in the competitive rewards-based shopping market. This project has identified significant vulnerabilities, including fraudulent account creation, redemption manipulation, and promo code abuse, which together contribute to millions in financial losses annually. The findings highlight the need for robust fraud detection and prevention measures to safeguard both Shopkick's financial health and user trust.

The proposed recommendations—ranging from enhanced account verification to tiered redemption thresholds—are designed to address these vulnerabilities effectively. By implementing these strategies, Shopkick can achieve a 75% reduction in fraudulent account creation, prevent annual losses of $71,000 in key areas, and significantly reduce fraudulent kick earnings and promo code redemptions. These measures not only mitigate risks but also reinforce Shopkick's commitment to providing a secure and enjoyable user experience.

Beyond immediate benefits, these initiatives will position Shopkick as a leader in fraud prevention within the rewards-based app industry. As fraud tactics continue to evolve, Shopkick must remain proactive, leveraging advanced technologies and continuous monitoring to stay ahead of emerging threats.

In conclusion, the adoption of these recommendations will not only curb fraudulent activities but also enhance Shopkick's operational efficiency, user trust, and market competitiveness, ensuring sustainable growth for the platform.

Respectfully Submitted by,

Daniel Ardila, Student Consultant, MS in Engineering Management, JHU

Sriaansh Sahu, Student Consultant, MS in Engineering Management, JHU

Sharvi Dadhich, Student Consultant, MS in Engineering Management, JHU

Chuyang Yu, Student Consultant, MS in Engineering Management, JHU

7. Acknowledgement

The results of this project would not have been possible without the following people. We appreciate the time that you have taken to meet with us to help us gather data, gain insights, solidify our direction, and refine our recommendations.

- Richard Froggatt, Head of Shopkick Operations, Trax Retail
- Sarah Jankowski, Director of Shopkick Marketing, Trax Retail
- AJ Marchese, Ad Operations and Analytics Manager at Shopkick, Trax Retail
- Madhura Abhyankar, Senior Product Manager at Shopkick, Trax Retail
- Marcus Truscello, DevOps and Infrastructure Engineer at Shopkick, Trax Retail
- Chris Gee, Data Analyst at Shopkick, Trax Retail
- Derek Couture, Influencer and Affiliate Marketing at Shopkick, Trax Retail
- Hardik Shah, Teaching Assistant, Center for Leadership Education, JHU
- Riyaa Jadhav, Teaching Assistant, Center for Leadership Education, JHU

This was an incredible learning opportunity for each of us and we thank you for the role that you have played in the success of this project.

8. References

[1] Investing.com. (December 2, 2024). Ibotta's SWOT analysis: Digital coupon firm's stock faces growth challenges. Retrieved from: https://www.investing.com/news/swot-analysis/ibottas-swot-analysis-digital-coupon-firms-stock-faces-growth-challenges-93CH-3755885

[2] Fetch. (n.d.). Fetch Rewards app surpasses 5 million daily active users. Retrieved from: https://business.fetch.com/newsroom/fetch-rewards-app-surpasses-5-million-daily-active-users

[3] Tracxn. (n.d.). Shopkick: Market share retention. Retrieved from: https://platform.tracxn.com/a/d/company/OAZESiWBzUQujLtEZouUwLm_UpLOr47wQjw1Asa3z8A/shopkick.com/marketshareretention

[4] Cap Times. (March 21, 2024). Fetch Rewards app turns first profit and prepares for hypergrowth. Retrieved from: https://captimes.com/news/business/fetch-rewards-app-turns-first-profit-and-prepares-for-hypergrowth/article_0b7f96ee-e6eb-11ee-ab03-3b5325b56fc4.html

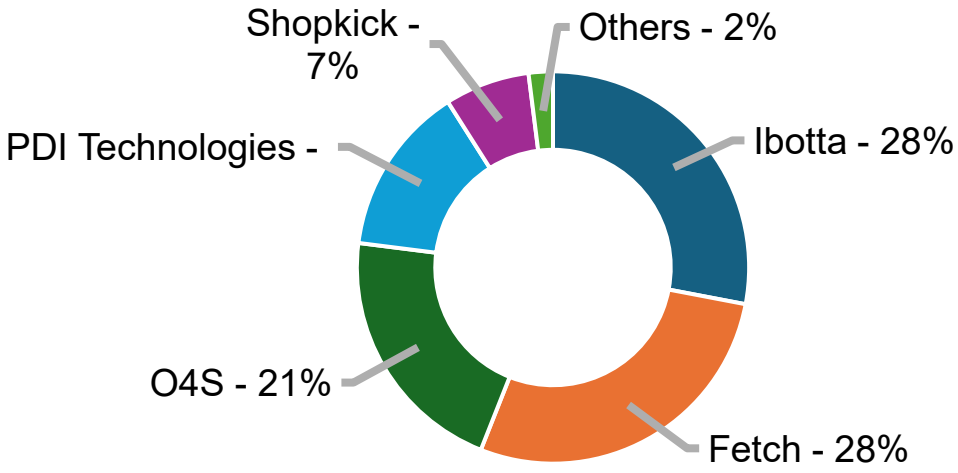
[5] The Motley Fool. (August 21, 2024). Ibotta vs. Fetch. Retrieved from: https://www.fool.com/money/personal-finance/ibotta-vs-fetch/

[6] Kount. (n.d.). Fetch. Retrieved from: https://kount.com/resources/customers/fetch

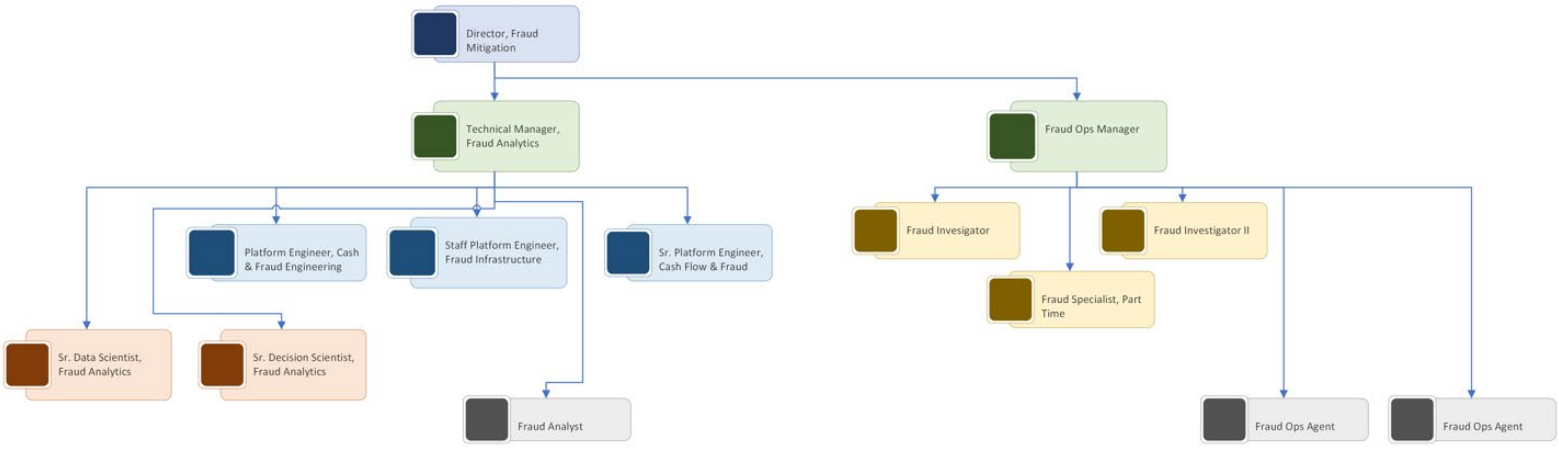
[7] Imply. (September 9, 2023). Combating fraud at Ibotta with Imply. Retrieved from: https://imply.io/blog/combating-fraud-at-ibotta-with-imply/

Appendix

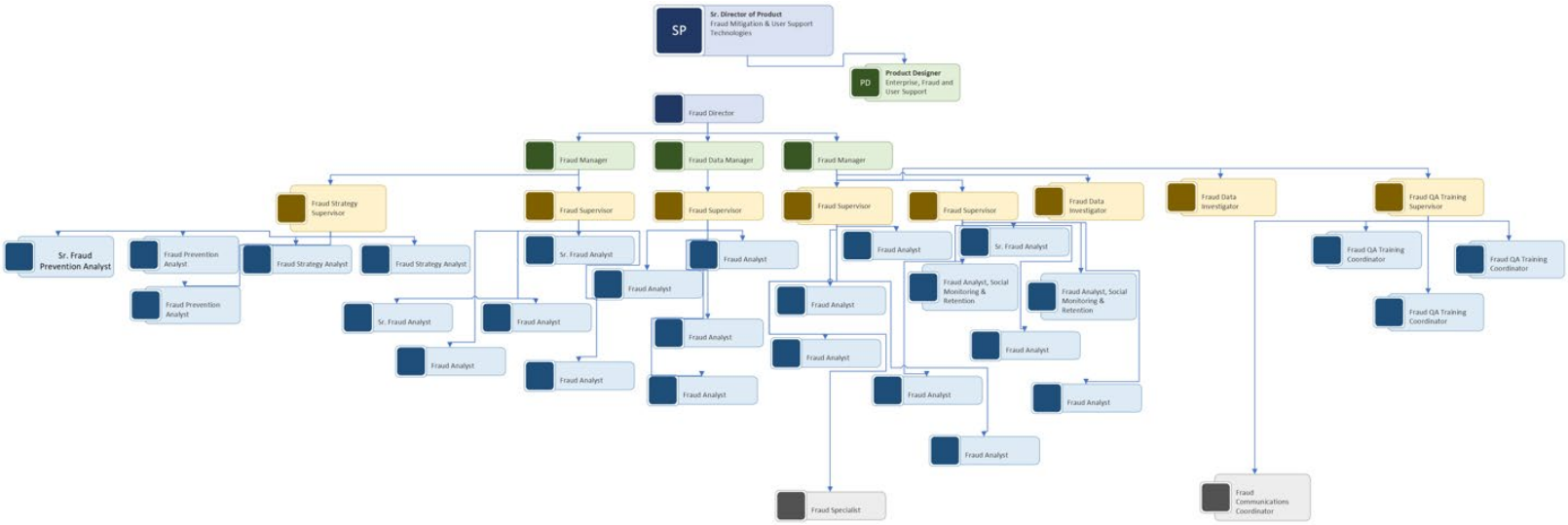
1. Market breakdown of shopping rewards apps in the U.S. – It is important to keep in mind that PDI and O4S are more data-focused companies rather than 'cash-back' companies.



2. Ibotta's fraud team – compiled by Shopkick from LinkedIn postings



3. Fetch's fraud team – compiled by Shopkick from LinkedIn postings



4. Complete list of Fraud Goals for 2025 – including JHU team recommendations in green and Shopkick's internal goals.

Rank	Topic	Effort	Current Methodology	Modification
1	Receipts - programmatic API integrations w/ retailers, follow up to see if items have been returned	High External Barriers	N/A	Partnerships with retailers
2	**Increase first redemption minimum to $10**	Low	Currently redemption for some gift cards begins at $2	Remove the option to redeem $2 and $5 on first redemption
2	**Phone Number Verification @ Start**	Low	Currently not done until redeeming, done by competitors	Ask for phone numbers, not a wholistic solution but will help
3	First X receipts go to SRTS	Medium	Currently all receipts are manually reviewedd	Combine these 3 processes
3	Random receipt sampling go to SRTS			
3	Send all of a specific user's receipts to SRTS			
4	**Bracketed Payout Verification**	High	Currently there is no increase in verifcation standards for high lifetime redemption	Add verification steps (to be determined through user surveying) to redemption process

5	**Promo Code Tracking and Replacement**	timing + manual supervision + real-time data	Currently only campaign limits exist for affiliate link use	Create data streams for link use and run predictions algorithms over some time scale
5	Promo Codes - need activation criteria that have paper trail (eg scans, receipts)	Very Low Effort	This change is about to be made in an update	N/A
5	Create single use unique promo code	High	Currently not supported	Create capability for unique promo codes
6	Credit/Debit Card Linking	High, including user reluctance	N/A	Research into financial implications, consumer willingess = transaction cost
7	Keep & maintain SIFT	Low	N/A	N/A
8	Increased redemption processing time	High	Currently limited to 10 attempts w/ 60 sec delay in the middle	Need a way to add manual review for redemptions within our system to tolerate a longer response time
9	Return Fraud	Unkown Barriers	Using store credit to purchase items results in kicks not rewarded	
10	Better barcode fraud detection - detecting image of screen	High	Currently done by software	Look for new software or create in house modifications

5. Competitors Analysis

Company	**Shopkick**	**Fetch**	**Ibotta**	**Upside**	**Rakuten**
Fraud Software	Sift	Kount (by Equifax)[2]	C.I.A & Imply[3]	In-House Software	In-House Software
Receipt Software	Blink	Blink	Blink	Debit/credit card	Debit or credit card
User base (# Millions)	~400,000 active monthly users	17 Million active users[8]	50 M registered[6] (as of 04/2024)	~35M consumers[20]	21 million users[13]

Value Proposition	Hands-on marketing through walk-ins and scans Allow brands to run campaigns	Gather data on consumer behavior Allow brands/retailers to run campaigns	1. Cashback (not points) 2. Scan the barcode anytime to check if there's an offer	Cashback on gas, restaurants, groceries in-app promotions, ads 27gift card options	Highly personalized, merchant-focused business model [15] [16]
Metrics	$2.2 million in fraud	$152bn in transactions[4] $900mil in rewards	$38 million net profit[6] 2700+ retailers[18] $800 million in rewards[18]		$2 billion in Q2 2024 [17]
Require a phone #	No	Yes	No	Yes	No
Can send promo w/o phone #	Yes	No	Yes	No	Yes
Currency	Kicks	Points	Dollars ($)	Dollars ($)	Dollars ($)
Time from receipt to currency	Kicks are immediately rewarded for scans and walk-ins Receipts are reviewed manually	Points for receipts go straight to your account - point values are low for large purchases (only points for offers)	Users' rewards will be sent within 24 hours after receipt submission[14]	10 days to process the receipt 24-48 hours to get funds in bank account[21]	Every 15th day of the month, once every 3rd month[10]
Time to receive gift card	Most are immediately available (can take a few hours depending on shopper traffic)[7]	3-day delay for "account security"	Immediately for PayPal/gift card 1-3 days for bank	immediately	Every 15th day of the month, once every 3rd month[10] (quarterly payments)
Redeem minimum	$5	$10 for the first time and after that you can redeem for $3, $5...[8]	$20	N/A	$5.01[10]
How long can you redeem a receipt for?	10 days	14 days[8]	7 days[12] Can only submit receipt after adding offers to list[9] Add offers-shopping-upload receipts	N/A	N/A
Require additional verification to redeem	Yes, must verify the phone number again	No	No	yes	Verify address[10]

How to earn points	Walk-ins, scans, purchases, videos, referrals	Receipts (e and paper), play apps, buy offers, refer a friend, point boost[11]	1. Redeem: link account/upload receipt 2. Bonus: depends on retailers (shop 3 times/redeem 2 offers…) 3. Referral	claim a nearby cashback offer, then make your purchase at that location and pay with a credit or debit card to earn rewards.	Shop at partnered stores and activate cashback. In-Store Cashback: Link your credit card on Rakuten, activate in-store offers
E-account linking	Not yet	Yes	Yes	yes	Yes
Bank Account Withdrawal	No	No	Yes	yes	Yes
Other notes	Lose kicks if inactive for more than 6 months	If inactive for 90 days, then your points expire	Inactive maintenance fee[5] Will deduct $3.99 per month from your earnings if you don't use the app for 180 days.		

6. Comparison of Key Features in Fraud Detection and Prevention Tools Used by Shopkick, Fetch, and Ibotta

Feature	Shopkick	Fetch Rewards	Ibotta
Fraud Detection Platform	Using Sift, leverages machine learning models and a global network processing 1 trillion events annually	Partnered with Kount, an all-in-one fraud prevention platform	Uses Apache Druid and Imply for real-time analytics
Key Approaches	Advanced Al-driven fraud detection with ThreatClusters technology	AI-driven fraud detection using supervised/unsupervised machine learning	Real-time anomaly detection analyzing behavior changes
	Customizable platform to fit specific business needs	90% reduction in manual reviews	A multifaceted strategy combining third-party and internal data
	Real-time detection and prevention for swift fraud identification	Improved automation for approvals while maintaining fraud control	Empowering non-technical users with fast investigation tools

	Lower chargeback rates (0.08%, 97% below the industry average)	Data transparency for insights into fraud patterns	Subsecond queries and no-code workflows for quick actions
		Custom risk thresholds and policies	
Key Results	N/A	70% reduction in fraud rate	Improved control over fraud attacks
		400% increase in active users while maintaining fraud control	Faster response to fraud and non-fraud issues
		Efficient scaling of fraud prevention operations	Reduced day-to-day usage of fraud detection tools
			Capability to address root causes and close fraud loopholes