

# Fraud Detection in Reward-Based Crowdfunding: A Framework for Identifying Fraudulent Campaigns

Author: Loran Knoop  
University of Twente  
P.O. Box 217, 7500AE Enschede  
The Netherlands

## ABSTRACT,

*Platforms for reward-based crowdfunding, such as Kickstarter, provide opportunities for innovation but also give a chance for possibly fraudulent behaviour. Through an analysis of two high-risk subcategories, tabletop games and high-tech gadgets, this study intends to identify characteristics that indicate campaign fraud. The independent variables, minimum reward, campaign duration, word count, spelling error percentage, and sentiment score, are investigated.*

*We manually verified 348 campaigns to conduct an analysis to determine whether they could be fraudulent. These campaigns were selected on the criterion that they did not enter the public market. To determine whether a crowdfunding campaign is considered fraud, five criteria are created: the minimum reward to receive a physical product is higher than the 80th percentile of all rewards, the funding period is longer than a month ( $\geq 32$  days), the word count of the description is below the 20th percentile, the percentage of spelling errors is greater than 3%, and the sentiment score of the description is negative. When at least three out of five criteria are met, the campaign is considered to be fraudulent.*

*This research contributes to theory in the crowdfunding field by addressing how fraud connects to observable campaign characteristics. Crowdfunding platforms, backers, and campaign creators can benefit from this model by identifying suspicious and fraudulent behaviour. Findings imply that the risk of a campaign being fraudulent is not random and can be predicted by using publicly available data.*

## Graduation Committee members:

Claire van Teunenbroek

Raymond Loohuis

## Keywords

Crowdfunding, Reward-Based Crowdfunding, Fraud, Fraud Detection, Kickstarter, Fraud Characteristics

*During the preparation of this work, the author used ChatGPT in order to assist with cleaning and coding of data in RStudio, and Grammarly in order to correct grammar and spelling. After using this tool/service, the author reviewed and edited the content as needed and takes full responsibility for the content of the work.*

# 1. INTRODUCTION

One well-known case of attempted crowdfunding fraud is “Kobe red beef jerky” on Kickstarter, a project by Magnus Fun Inc., which claimed to provide fresh Kobe beef-based jerky from Japan and posted fake user experiences showing they loved the taste. It almost enabled a \$120,309 heist, nearly 50 times the original financing goal of the campaign, from 3252 backers (i.e., donors) in just less than 1 month. Fortunately, Kickstarter pulled the plug on this fraud at the last minute of the fundraising period (Lee et al., 2022).

The Cambridge dictionary defines crowdfunding as “*the practice of getting a large number of people to each give small amounts of money in order to provide the finance for a project, typically using the internet.*” The most obvious advantage of crowdfunding for a start-up company or individual is its ability to provide access to a larger and more diverse group of investors or supporters. With the ubiquity of social media, crowdfunding platforms are a useful strategy for businesses and individuals to both grow their audience and receive the funding they need (Smith, 2024).

There exist different types of crowdfunding. Equity-based crowdfunding allows crowdfunders to invest in a crowdfunding project in exchange for shares or profit of the unlisted company. Peer-to-peer lending (sometimes called crowdlending) is a direct alternative to a bank loan, with the difference that, instead of borrowing from a single source, companies can borrow directly from tens, sometimes hundreds, of individuals who are ready to lend. Crowdlenders often bid for loans by offering an interest rate at which they would lend. Borrowers then accept loan offers at the lowest interest rate (European Union, n.d.). Donation-based crowdfunding is based on donations without any expected return. Reward-based crowdfunding offers rewards in return for funding a project (Yacoub et al., 2022). Typically, donation-based platforms (e.g., GoFundMe) thrive on giving behaviour as a rule, while reward-based platforms (e.g., Kickstarter) allow donations in the “reward” tiers (van Teunenbroek et al., 2023). On the platform Kickstarter, creators choose the length of the funding campaign, funding goal, and reward tiers, and these cannot be altered once the campaign has started. The different tiers list the rewards that are given in exchange for pledges, and the minimum pledges necessary for each tier. Almost all projects feature multiple reward levels to accommodate backers contributing different amounts (Qiu, 2013). This research will focus on reward-based crowdfunding, as it is the most popular type of crowdfunding that is available for startups (University Lab Partners, 2020). Reward-based crowdfunding consists of individuals donating to a project or business with the expectation of receiving a non-financial reward in return, such as goods or services at a later stage. A common example is a project or business offering a unique service (rewards) or a new product (pre-selling) in return for investment. This form of crowdfunding allows companies to launch with orders already on the books and cash-flow secured (a major issue for new businesses), and gathers an audience before a product launch (European Union, n.d.-b).

Unfortunately, some of these crowdfunding campaigns are scams. Cumming et al. (2023) identified 193 fraudulent campaigns on Kickstarter between 2010 and 2015. Perez et al. (2022) collected a dataset with over 700 crowdfunding campaigns, of which they labelled 292 as definitely fraudulent. The sample of Mollick (2014) states that 2,3% of projects showed indications of potential fraud. Since donation-based and reward-based crowdfunding platforms verify less rigorous than on equity- and lending-platforms, reward-based backers are more vulnerable to fraud, making transparency and platform

accountability critical concerns (Machado et al., 2024). Macari & Chun Guo (2021) state that, unlike equity and debt-based crowdfunding, reward-based crowdfunding transactions lack detailed legal contracts and extensive regulation. Therefore, they are subject to violations of the terms of use, especially when it comes to the requirement to complete the project and fulfil each reward. Reward-based crowdfunding platforms collect the money from pre-ordering buyers and transfer all the funds to the entrepreneur if the target is met, returning them if not. This creates an opportunity for fraud as the entrepreneur could pocket the aggregate funds pledged, forego production to save her costs, and disappear without delivering the product (Ellman & Hurkens, 2019).

According to the legal dictionary from law.com, fraud is defined as “*the intentional use of deceit, a trick or some dishonest means to deprive another of his/her/its money, property or a legal right.*” In the field of reward-based crowdfunding, Cumming et al. (2023) categorize fraud into two categories: detected fraud and suspected fraud. The first category, detected fraud, includes pre-empted fraud and attempted fraud. Pre-empted fraud occurs when a supposedly fraudulent crowdfunding campaign is closed down before any money is transferred to the creator’s account, just like in the aforementioned “Kobe red beef jerky” example. This can occur, for example, when warnings are posted online that the campaign carries a risk of fraud. Attempted fraud happens when fraud was not originally detected during the campaign’s funding period, and the campaign creators obtain the amounts raised. When the campaign is finished, backers may find out that the project was fake and that they lost their money. The second category, suspected fraud, occurs when a supposedly fraudulent campaign is reported in the media and three specific conditions are met simultaneously, or when the rewards are changed to the disadvantage of backers. The three conditions are: rewards are delayed by more than one year from the promised delivery date, the creators cease credible communications with backers for at least 6 months after the promised delivery date, and rewards are not delivered, and backers have been neither partially nor fully refunded (Cumming et al., 2023). However, it is not uncommon for founders to delay rewards or provide no rewards at all. Reasons for this can include procurement problems, regulations, reward complexity, shipping costs, or campaign cancellation. Delays can also occur due to unexpected volume: when founders raise far more money than anticipated (Hossain & Creek, 2021). This means that it is difficult to draw the line between a fraudulent campaign and a failed campaign that did not anticipate a major success or did not take into account any setbacks that might occur.

Kickstarter is the largest reward-based crowdfunding platform. Since its launch in 2009, over 24 million people have backed a project, more than 8,6 billion US dollars have been pledged, and over 275,000 projects have been successfully funded. 9% of all Kickstarter projects failed to deliver rewards (Kickstarter, n.d.). As mentioned before, there can be multiple reasons for not receiving a reward, so this means that not all of those failed projects are actually scams. However, Appio et al. (2020) state that KickScammed provides us with a more dramatic picture: more than 50% of projects do not deliver the promised rewards to backers, and there is around \$3 million in ‘scams’ in the crowdfunding context.

## 1.1 Problem statement

Reward-based crowdfunding has increased in popularity as a form of raising funds over the years. Unfortunately, this increasing popularity also brings negative consequences. The number of fraudulent campaigns increases as well, which has an impact on the trust of potential backers of projects. Although

platforms try to avoid publishing fraudulent projects and remove them when necessary, the lack of a strict verification process makes it difficult to fully protect backers from scams. In order for backers to check whether a project is legitimate, a framework should be created. Although some websites mention some guidelines and common sense to notice red flags, a coherent, clear framework to detect fraudulent crowdfunding campaigns does not currently exist.

## 1.2 Research objective and question

This thesis aims to gain a better insight into the number of fraudulent reward-based crowdfunding campaigns and to give backers an estimate of whether a crowdfunding campaign could be fraudulent. This helps prevent backers from spending their money on campaigns that will most likely not deliver the promised rewards. The objective of this research is to detect if there is a relationship between a certain reward-based crowdfunding category and the number of fraudulent campaigns within that category. To reach this objective, the following research question is formulated: **“Which reward-based crowdfunding categories are most vulnerable to fraud?”**

To be able to answer this research question, the following sub-questions should be answered:

- *“What factors characterize fraudulent crowdfunding campaigns?”*
- *“How do fraud rates differ between crowdfunding categories?”*

## 1.3 Academic and practical relevance

The academic relevance of this research is to expand the knowledge of fraudulent activities in reward-based crowdfunding. Previous research mainly focused on the risks of investing in a certain project in terms of whether the project is expected to fail or succeed. For example, the research of Mollick (2014) shows that among reward-based crowdfunded projects, failures happen in large amounts, successes in small amounts. Projects that fail tend to fail by large margins. The mean amount funded of failed projects is 10.3% of the goal. Only 10% of projects that fail raise 30% of their goal, and only 3% raise 50% of their goal. Yasar et al. (2022) show that only 41% of projects are successful. The overall success rate of 41 % also varies among categories, with the games category having the highest success rate (49 %) and the technology category having the lowest (29 %). Around one-third of the projects in our sample exceeded their goals by 10 % or more. However, there is a lack of research on the likelihood of fraud within crowdfunding. This research adds value to the contribution of knowledge of fraud within the crowdfunding field.

By identifying patterns and factors that are characteristic of fraudulent campaigns, the findings of this research can give a better understanding of how fraud prevention techniques can be optimized and/or adapted to more accurately determine if a project is a scam or just poorly designed. The findings of this research can be practically relevant for backers and crowdfunding platforms to detect fraudulent campaigns. Backers can establish which campaigns have a higher risk of being fraudulent and base their decision on whether or not to invest in the project. The findings of this research can also be useful for crowdfunding platforms. If a certain campaign has a high probability of being fraudulent, the platform can take action and investigate the campaign to determine if it is a legitimate project or a scam. Finally, the findings can be of practical relevance for the creator of a crowdfunding campaign as well. If a project is marked with a high probability of fraud, the creator can improve

his/her structure/design/description of the campaign in order to gain more trust from potential backers.

## 2. LITERATURE REVIEW

This section looks into theoretical and empirical perspectives on fraud in crowdfunding. we begin by assessing who is responsible for fraud prevention and detection between crowdfunding platforms and backers, after which we discuss several different factors related to fraud in the crowdfunding field.

### 2.1 Responsibility

While it is the responsibility of the crowdfunding platforms, they seem to struggle with fully preventing fraudulent behaviour on their platforms.

Although it is the responsibility of crowdfunding platforms to prevent fraudulent behaviour, backers should also be able to detect red flags of a crowdfunding campaign and detect fraudulent behaviour. Crowdfunding platforms already take measures to prevent fraud on their platform. For example, Kickstarter has a Trust & Safety team that monitors the system for suspicious activity. They screen the reports that are sent to them by the community and take action if they find something that does not align with their rules. Whenever a project is reported by a backer, the Trust & Safety team will perform a full review. Kickstarter encourages its users to report the projects they believe violate any rules (Kickstarter, n.d.). This means that detecting fraud is partly the responsibility of the backers. When backers have doubts about a campaign, they can, for example, ask questions to the project creator or do a social media check to see if the creator of the campaign is a real person with a real campaign that can be trusted. GoFundMe offers a checklist that can be used to recognize fraudulent campaigns. This means that, at the end, the backers of a campaign are responsible for determining whether the campaign is valid or not. In case a campaign turns out to be fraudulent, GoFundMe offers a refund of any amount donated up to one year after the donation has been made (GoFundMe, n.d.). The creation of the model in this research will give backers an extra safety tool to determine whether or not to trust a crowdfunding campaign.

### 2.2 Fraud prevention

Avoiding fraud saves time and financial resources, since detecting it after it occurs has the consequence that the stolen assets are practically irrecoverable. To enhance fraud prevention, organizations should focus on the root of the problem by identifying the causes that lead people to commit fraud and understanding their behaviour. The most frequently used theories in fraud prevention are the Fraud Triangle Theory (FTT) and the Diamond Fraud Theory (DFT). The Fraud Triangle Theory was proposed by Donald R. Cressey (Kassem, 2012). Cressey investigated why people committed fraud and determined their responses based on three elements: pressure, opportunity, and rationalization. This theory also mentions that these elements occur consecutively to provoke the desire to commit fraud.

The first necessary element is perceived pressure, which is related to the motivation and drive behind the fraudulent actions of an individual. This motivation often occurs in people who are under some form of financial stress. The second element, perceived opportunity, is nothing more than the action behind the crime and the ability to commit it. The third component, known as rationalization, has to do with the idea that the individual can rationalize their dishonest acts, making their illegal actions seem justified and acceptable. The FDT, considered an extended version of the FTT, integrates a new vertex with the three that were already known: capacity. Despite the cohesion among the three vertices of pressure, opportunity, and rationalization, it is

unlikely that people will commit fraud unless they have the capacity. The potential perpetrator must have the skills and ability to commit fraud (Sánchez-Aguayo et al., 2021).

In addition to the Fraud Triangle Theory, the Signalling Theory (Spence, 1973) suggests that individuals aim to show credibility in order to reduce information asymmetry. Campaign creators use signals, such as the description, communication, and previous success, to show quality. Fraudulent campaigns might create false signals or avoid clear signals to mislead backers.

### 2.3 Fraud detection in crowdfunding

The process of fraud detection in crowdfunding campaigns involves the application of data-centric strategies to spot atypical characteristics indicative of fraud. Through the examination of patterns and trends within extensive datasets, these platforms can identify discrepancies that stray from normal behaviour. Recent advancements in AI and predictive modelling have significantly improved the ability to detect fraud dynamically. Implementing robust fraud detection protocols allows platforms to avert such fraudulent activities, ensuring equitable practices and compliance with regulatory frameworks.

Several studies are researching blockchain technology as a valuable option against crowdfunding fraud (Machado et al., 2024). However, the algorithms are not complete yet, and therefore cannot be used at the moment. Blockchain is a database of records of transactions that is distributed, and which is validated and maintained by a network of computers around the world. Instead of a single central authority such as a bank, the records are supervised by a large community, and no person has control over it, and no one can go back and change or erase a transaction history. This is in line with the process of crowdfunding, since crowdfunding does not have a central authority. Blockchain allows anyone on the network to access everyone else's entries, which makes it impossible for one central entity to gain control of the network (Sarmah, 2018). The system created by Kumar et al. (2023) is a great example of how blockchain can be used for fraud prevention. Their Ethereum Smart Contracts-Blockchain would result in a considerable decrease in scams and make it a trustworthy payment system, which would also attract more audience. When a campaign is created, the campaign information will be managed by the Ethereum-based smart contract and thus cannot be tampered with. Once a campaign has been created, users can share the campaign, and anybody can contribute to the campaign. The funds will go to the address of the campaign and not to the creator of the campaign, thus making the process more efficient and anti-fraudulent. The creator of a campaign can propose how to use the funds in the form of a spending request. The creator of the campaign can describe their spending request and add the address of the wallet to which the creator wants to send money. Anybody who contributes more than a particular amount is called an approver and will be able to approve or deny the request. This system will make sure that the funding is used in a proper manner and way and will also make sure that on which particular part, the portion of funding is spent. This means that donors/funders of a crowdfunding campaign gain more control of the money they donated/funded, since creators of the project cannot spend the received money on just anything they want. Donors/funders first have to approve the request of the creator before the money is sent to the wallet of that request. In this case, the money received from the crowdfunding campaign will never directly go into the pocket of the creator.

Several researchers (Baber, 2020; Hartmann et al., 2019; Nguyen et al., 2021) propose using Blockchain Technologies (BT) as they can revolutionize the crowdfunding industry by increasing transparency, security, and efficiency. Blockchain can be used in

crowdfunding to automate the distribution of funds and rewards, reducing the need for intermediaries and increasing transparency. BT could also be used to verify the identities of campaign creators and backers, helping to reduce the risk of fraud and increase trust (Zkik et al., 2024). Finally, Blockchain increases the democratization, since funders have more control over the allocation of the funds. The development of BT in the crowdfunding field sounds promising. However, it is not yet ready to be applied in practice. That is why this paper focuses on identifying fraudulent crowdfunding campaigns based on their project characteristics. The purpose is to develop a framework that potential funders can use as a guideline to determine if a campaign is fraudulent.

### 2.4 Time-frame

Cumming et al. (2023) observe that more confident creators restrict the funding period duration because they believe their projects will be funded rapidly. But fraudsters are less likely to send credible signals of quality. So they may tend to extend the funding period to raise as much capital as possible. Longer funding periods may make detection more likely and increase the risk of not receiving funds. Cumming et al. (2023) believe that a short funding period is a credible signal of project quality, and perceived project quality is an important factor in reward-based crowdfunding (van Teunenbroek & Bekkers, 2020). Koch & Siering (2015) conclude that the influence of the funding period length was not shown to be significant, which can lead to the conclusion that platform members who are interested in a campaign place their funding within the first days after the campaign has become public, so that a longer funding period does not lead to further advantages.

**Hypothesis 1:** Time frame will be positively related to the chance of a campaign being fraudulent.

### 2.5 Height of the reward

Some rewards offered to potential backers can be overpromising and underdelivering. They might not always be fraudulent, but some campaigns offer unrealistic rewards that they cannot fulfil. Rewards that are too good to be true might be a sign of fraudulent behaviour. Chakraborty & Swinney (2021) find that a low reward price is a signal of campaign quality. This suggests that backers are more likely to trust campaigns that offer modest, reasonable awards. Furthermore, campaigns that require a high minimum pledge to receive a physical reward may be covering up the fact that their product is hard to produce, thereby hiding the underlying risks from potential backers.

**Hypothesis 2:** The minimum height of a reward to receive a physical product will be positively related to the chance of a campaign being fraudulent.

### 2.6 Campaign description

In crowdfunding markets, fraudulent campaign creators may try to increase information asymmetries to make it more difficult for backers to differentiate between scams and worthwhile projects. The main way to convey information about a project is through the description, which is normally a few thousand words. Crowdfunding fraudsters are, therefore, less likely to provide a professionally worded description in order to foster confusion and avoid detection. In contrast, professional entrepreneurs are likely to use campaign descriptions to signal quality (Cumming et al., 2023).

During their research, Li & Qu (2022) found that some ideas from the method of fake news detection can be applied to the research of detecting fraudulent crowdfunding projects. For example, a method of fake news detection based on article information. Text information extraction can help us learn more about crowdfunding projects, which can help us further research

the detection of fake crowdfunding projects. The important information in the text can generally be reflected in the keywords. However, extracting crowdfunding project information alone cannot help to identify fraudulent crowdfunding projects, since fraudsters try to write a convincing description to mislead possible investors. This is why Li & Qu proposed a comprehensive method to identify fraudulent crowdfunding projects. The method proposed by the research first extracted the keywords of the crowdfunding project and then retrieved the characteristic information of the crowdfunding campaign to obtain the judgment basis of the fraudulent crowdfunding project. Finally, machine learning algorithms were used to classify the authenticity of crowdfunding projects. The main methods for the detection of fake crowdfunding projects are divided into two categories: First, the language approach, language patterns linked to false (contradictory); Perez-Rosas, who proposed a language method to detect conflicts. Second, the network method uses network information to fake (contradictory) connections.

**Hypothesis 3a:** The number of words in the description will be negatively related to the chance of a campaign being fraudulent.

**Hypothesis 3b:** The percentage of spelling mistakes will be positively related to the chance of a campaign being fraudulent.

**Hypothesis 3c:** The sentiment analysis will be negatively related to the chance of a campaign being fraudulent.

### 3. METHODOLOGY

To study the difference in fraud rates among reward-based crowdfunding categories, this research focuses on secondary data and manual data scraping. This section explains the data collection, cleaning, processing, and analysis of this quantitative data.

In this study, we focus on comparing two types of crowdfunding categories. The two categories that will be evaluated during this research are tabletop games and high-tech gadgets (hereafter referred to as 'gadgets'). Tabletop games and gadgets are subcategories of the parent categories, games and technology, which are both in the top 3 most funded categories (Kickstarter, n.d.). Since most money is spent in these categories, it makes them attractive for scammers.

#### 3.1 Data selection and collection

In this study, we combine two datasets: (1) tabletop games, and (2) gadgets.

*Tabletop games.* In this step, we collected project characteristics of the Tabletop games. To do this, two broad steps were undertaken to select the included projects. First, using a general dataset of Kickstarter projects, we selected all projects that followed the following criteria:

- Time: Datasets were collected from the months of June 2019 and December 2020. Since projects can have a duration of up to two months, the decision was made not to collect datasets of two consecutive months to avoid having duplicate projects.
- Category: Tabletop games.
- Country: US.
- Currency: US dollars (to double check all projects are American, since some projects set their location in the US, while pledges had to be paid in Hong Kong Dollars).
- Status: Successful (to make sure the project achieved its funding goal). This means that the campaign is finished with total pledges equal to or higher than the funding goal.

This selection was applied to a pre-existing dataset shared via webrobots.io.

This selection resulted in a dataset containing 1848 Tabletop game projects.

Second, we applied another selection round to focus only on projects that did not reach the market. This selection was done manually via an extensive Google search. Each project was manually assessed to determine whether the central product was available on the public market.

In this research, a product is considered to be publicly available if it can be purchased by someone who is not connected to the original crowdfunding campaign. If a product was previously sold on a platform like Amazon but is now out of stock or no longer listed, it is still regarded as publicly available. Blogs, reviews, and Reddit pages about the product were also checked to find links to stores where the product could be bought. In case the product is offered on eBay, it is evaluated carefully. A product found on eBay is not automatically considered publicly available, since it could be a used item obtained as a reward from the crowdfunding campaign. In those cases, the product is not counted as publicly available. However, if the product is listed as new and sold by a retailer with multiple units in stock, it is assumed to be publicly available.

It took a substantial amount of time (70-80 hours) to collect data that describes whether a product was publicly available, since each product had to be manually verified. If no (reliable) information about the product could be found within five minutes of searching, the project was marked as not publicly available. After the 1848 campaigns were manually checked, we decided to continue with the analysis to spend the remaining time in a valuable manner. Out of these 1848 campaigns, only 168 were not publicly available. After double-checking these campaigns and removing duplicates, 162 tabletop games were selected for further analysis.

*Gadgets.* The second dataset, which contains projects in the category "gadgets", was received from Dr. Claire van Teunenbroek. This dataset includes 300 projects, all of which are marked as successful in terms of completing the crowdfunding campaign on Kickstarter.

Since this dataset already contains the variable "market entry, the data needed only to be filtered by the criteria "Country: US", "Currency: US dollars," and "market entry: no". This resulted in a total of 186 projects available for the analysis. It is important to note that the selection process of determining if a project was unsuccessful in reaching the market was the same for both datasets: tabletop games and gadgets.

#### 3.2 Web-scraping

To be able to conduct the analysis, the following variables are web-scraped from each campaign page:

1. **Height of the reward.** Each reward-based crowdfunding campaign has a minimum amount that needs to be pledged in order to receive a reward. Sometimes there are multiple "levels" of rewards. This variable will show the minimum amount that should be pledged in order to receive a reward. Only physical products are considered as a reward. Many projects offer the option to only donate \$1 as a gift in return for a virtual hug or a personalized thank-you email. These are not considered a reward, so in those cases, we take the next level of rewards that is considered physical. Rewards that could be turned into a physical reward are also sufficient. For example, especially in the tabletop category, there are a lot of print-and-play or 3D printable rewards. The

backer receives a file that can be printed at home and turned into a physical product.

2. **Description.** The description of each project is collected to create more variables later on. Only the section “Story” is collected from each campaign. Some descriptions also have sections “environmental impact” and “risk and challenges”. However, this is not the case for all projects. To keep all descriptions equal, only the “Story” section is included.
3. **Title.** The title of the campaign is needed to conduct a proper analysis of the description.
4. **Start and End date.** These are needed to calculate the funding period, since it was not possible to web scrape the data field “funding period”.

Since the dataset gadgets already contained the variables title and start, and end date, we only web-scraped the variables height of the reward and description for the gadget campaigns.

The web scraping is performed using the application Octoparse, which is a data extraction tool. A URL of a single Kickstarter project is entered in the program, and the variables mentioned above are selected. All variables are automatically web-scraped from the Kickstarter project page. Once the program knows which variables to extract from the project page, a list of all 168 URLs from tabletop projects was pasted into Octoparse, and it automatically generated an Excel file with a table with all variables. This process was repeated for the 186 gadget projects. Some missing data was added into the blank cells after manually looking it up in the corresponding project.

### 3.3 Analysis

#### 3.3.1 Calculating missing variables

Both datasets (tabletop games and gadgets) were imported and analysed in RStudio. However, before starting the analysis, some missing variables needed to be calculated.

- a. **Number of words in the description.**
- b. **The sentiment of the description.** This will show whether the description is written in a positive, neutral, or negative sentiment. Examples of words that are used for the sentiment analysis are “happy”, “excited”, or “embarrassed”. This will be calculated by using the sentiment analysis available in RStudio.
- c. **The number of spelling errors in the description.** Since Kickstarter is an American platform and the majority of the campaigns are from the US, we will use the vocabulary/dictionary from the US for this variable. Since product names are usually non-existent words, they are often flagged as misspelled. To avoid this problem, all words from the project title that are flagged as misspelled are excluded from the spelling error count. Also, all emoticons and punctuation are removed. This is done to avoid cases where the last word of a sentence is flagged as misspelled, because it ends with a period. This means that the spelling checker would count “period.” as misspelled, simply because there is a period attached to the word. Finally, since the word “Kickstarter” is not in the American dictionary, we manually added it so it won't be marked as misspelled.

- d. **Spelling errors as a percentage of the total number of words.** This is calculated with the following formula:  

$$((\text{number of spelling errors}) / (\text{total words})) * 100.$$
- e. **Funding period.** It was not possible to web scrape this variable. This variable is obtained by calculating the delta between the start and end dates.

Now that all independent variables are collected, we can create a formula to calculate the dependent variable, which is possible fraud. First, the variable points\_fraud was created with a scoring range between 0 and 5. The score was assigned via a checklist: One point is added to this variable for each of the following conditions:

- The minimum reward of the project is higher than the 80<sup>th</sup> percentile of all minimum rewards within the campaign's category.
- The duration of the project is longer than a month ( $\geq 32$  days).
- The word count is lower than the 20<sup>th</sup> percentile of all word counts within the projects category.
- The percentage of spelling errors is more than 3%. Research from Flor et al. (2015) the average native person has a spelling error percentage of about 2,3%. Since the descriptions of the projects contain abbreviations such as USB or Wi-Fi, which are correct in the context, but are marked as misspelled by the spelling checker, we round the average spelling mistakes up to 3%.
- The score of the sentiment analysis equals -1, since a negative sentiment is a characteristic of fraud.

Finally, the variable possible\_fraud is created. Whenever a project has a value of 3 or higher (so more than half of the criteria are met) for the variable points\_fraud, we mark the project as possible fraud.

#### 3.3.2 Types of analyses conducted

Several statistical analyses will be conducted to assess the relationship between campaign characteristics and the likelihood of fraud. First, a chi-square test of independence will be used to compare fraud rates between the Tabletop Games and Gadgets categories and to determine whether the datasets can be analysed in a singular, combined model or should be analysed separately.

A descriptive analysis will summarise the key values of the independent variables: minimum reward, funding duration, word count, percentage of spelling errors, and sentiment score. The Shapiro-Wilk test will be used to check whether the data for each variable follows a normal distribution.

Next, a logistic regression analysis will be conducted to model the relationship between the independent variables and the binary dependent variable, possible fraud. Finally, the performance of the regression model will be evaluated using a Receiver Operating Characteristic (ROC) curve and the Area Under the Curve (AUC) metric, which assesses the model's ability to distinguish between fraudulent and non-fraudulent campaigns.

### 4. RESULTS

This section explains the findings from the analyses of the datasets tabletop games and gadgets. The goal is to evaluate whether the campaign characteristics identified in the theory section are significantly related to the likelihood of a campaign

being marked as potentially fraudulent. By comparing the results between the tabletop games and gadgets categories, this section also investigates whether fraudulent behaviour occurs differently across these categories. A framework is created to detect fraudulent campaigns based on easily observable campaign characteristics.

We begin by comparing the fraud rates across both categories using a chi-square test of independence. This reveals whether the datasets can be combined or should be analysed separately. Next, we conduct a descriptive analysis to summarize the key characteristics of the data, followed by the Shapiro-Wilk test to assess normality. A logistic regression is then used to test the hypotheses and identify which campaign characteristics have a significant relationship with potential fraud. Finally, the model's predictive ability is evaluated using the ROC AUC, which measures its accuracy in distinguishing fraudulent campaigns from legitimate ones.

#### 4.1 Chi-square test

A chi-square test is performed to determine whether the difference in fraud rates between the two categories is statistically significant. 10 out of 162 (6.17%) tabletop game campaigns were marked as fraudulent, while 28 out of 186 gadget campaigns (15.05%) were marked as fraudulent. The chi-square test results in an x-squared value of 6.14 and a p-value of 0.013. This indicates a statistically significant difference in fraud rates between tabletop games and gadgets. So, the likelihood of fraud is not evenly distributed across the two categories, and we need to test both categories separately.

#### 4.2 Descriptive analysis

The descriptive analysis provides an overview of the key values of all independent variables in both categories. As can be seen in Table 1, campaigns from the category gadgets take on average longer than the tabletop games campaigns. Campaigns from the category gadgets have a much higher average minimum reward than campaigns of the tabletop games category. The sentiment score shows that the descriptions of gadget campaigns are more often positively written than the tabletop games, while tabletop games have fewer spelling errors in their description than gadgets. Finally, gadgets have, on average, a longer description than tabletop games.

**Table 1. Descriptive Statistics of Campaign Characteristics per Category.**

Independent variable	Statistic	All (n=348)	Gadgets (n=186)	Tabletop Games (n=162)
duration (days)	M	32.69	36.60	28.20
	SD	10.35	9.15	9.84
	Mdn	30.00	33.00	30.00
minimum reward	M	44.53	66.95	18.79
	SD	59.94	71.51	24.87
	Mdn	21.00	41.00	12.00
sentiment score	M	0.82	0.96	0.67
	SD	0.54	0.26	0.71
	Mdn	1.00	1.00	1.00
spelling errors (pct)	M	2.15	2.28	1.99
	SD	1.42	1.38	1.44
	Mdn	1.88	2.06	1.72
word count	M	994.97	1055.86	925.05
	SD	675.57	592.25	755.92
	Mdn	859.50	958.00	683.00

Note: M = mean, SD = standard deviation, Mdn = median. Sentiment score 1 = positive, 0 = neutral, -1 = negative.

#### 4.3 Shapiro-Wilk test

Histograms of all variables from both categories can be found in appendix 6.1 and 6.2. Via this, we observe that not all variables are normally distributed. To test how closely the data matches a normal distribution, we use a Shapiro-Wilk test.

In this test, we focus on the W-value: The closer the W value is to 1, the more normally distributed the data is. A value closer to 0 means that the data deviates from a normal distribution. The p-value explains whether the deviation is statistically significant. If the P-value is lower than 0.05, the assumption of normality is rejected. In this case, all p-values are far below 0.05, which means none of the variables are normally distributed. A W-value close to 1 usually means the data looks like it is normally distributed. A p-value of <.001 means that the Shapiro-Wilk test rejects normality, indicating that the data is significantly different from normal. An example could be the min\_reward from tabletop games. The W-value equals 0.564, which would suggest a moderate normal distribution. However, when we look at the histogram of min\_rewards in Appendix 6.1, we see that the data is skewed to the right and is indeed not normally distributed. This justifies the use of Spearman's correlation instead of Pearson's correlation.

**Table 2. Shapiro-Wilk test for Tabletop games (n = 162) and Gadgets (n = 186)**

Dataset	Variable	W	p-value
tabletop	min_reward	0.564	<.001
tabletop	duration_days	0.909	<.001
tabletop	word_count	0.892	<.001
tabletop	spelling_error_pct	0.925	<.001
tabletop	sentiment_score	0.488	<.001
gadgets	min_reward	0.748	<.001
gadgets	duration_days	0.878	<.001
gadgets	word_count	0.944	<.001
gadgets	spelling_error_pct	0.927	<.001
gadgets	sentiment_score	0.124	<.001

Note: W = test statistic for the Shapiro-Wilk test of normality. W close to 1 indicates that the sample data is more likely to be normally distributed. W closer to 0 suggests that the data deviates significantly from a normal distribution.

#### 4.4 Hypothesis Testing

In this section, hypotheses 1 to 3c are tested by using a logistic regression model. The goal is to test whether the campaign characteristics have a significant relationship with the likelihood of a campaign being marked as fraudulent. The logistic regression is conducted separately for both the tabletop games dataset and the gadgets dataset to discover whether the results differ between the two categories. By analyzing both categories individually, we aim to discover category-specific trends. The results from the logistic regression will help to assess whether the data supports the hypotheses or not.

##### 4.4.1 Logistic regression

For this study, we use a logistic regression model instead of a linear regression model, since the dependent variable has a binary value. The logistic regression model is used to predict the chance that a project is being marked as fraud based on the values of the independent variables. Tables 3 and 4 show the logistic regression models of tabletop games and gadgets, where all independent variables are entered together in a single logistic regression model. These models are used to determine the relationship between campaign characteristics and fraud. The Estimate ( $\beta$ ) represents the strength and direction of the relationship between each independent variable and the dependent variable. The Standard Error (SE) measures how precise the Estimate is. So, if you repeat the research multiple times, the Standard Error shows how much the Estimate might vary during those multiple other researches. The z value shows



how strongly the predictor is related to the outcome in the model, relative to the error.

To determine the relationship between the independent variables and fraud, we follow the next benchmarks:

- Absolute Estimate < 0.30: weak relationship
- Absolute Estimate 0.30 – 0.60: moderate relationship
- Absolute Estimate > 0.60: strong relationship

The results from the logistic regression, which are shown in Table 3 (Tabletop Games) and Table 4 (Gadgets), provide an understanding of how various campaign characteristics relate to the likelihood of fraudulent behaviour.

#### 4.4.1.1 Minimum reward

We hypothesized that the minimum height of a reward to receive a physical product will be positively related to the chance of a campaign being fraudulent. This hypothesis is supported by the data. The minimum reward has a weak, significant positive relationship with fraud for tabletop games ( $\beta = 0.04$ ,  $n = 162$ ,  $p = .019$ ) as well as for gadgets ( $\beta = 0.01$ ,  $n = 186$ ,  $p = .040$ ).

#### 4.4.1.2 Funding period

We hypothesized that the time frame will be positively related to the chance of a campaign being fraudulent. This hypothesis is supported by the data. The duration of the campaign has a weak, significant positive relationship with fraud for both tabletop games ( $\beta = 0.12$ ,  $n = 162$ ,  $p = .004$ ) and gadgets ( $\beta = 0.11$ ,  $n = 186$ ,  $p < .001$ ).

#### 4.4.1.3 Word count

We hypothesized that the number of words in the description will be negatively related to the chance of a campaign being fraudulent. This hypothesis is partially supported by the data. The word count has a very weak, significant negative relationship with fraud for the tabletop games ( $\beta = -0.002$ ,  $n = 162$ ,  $p = .028$ ). However, the logistic regression shows a very weak, insignificant negative relationship with fraud for gadgets ( $\beta = -0.001$ ,  $n = 186$ ,  $p = .078$ ).

#### 4.4.1.4 Spelling errors

We hypothesized that the percentage of spelling mistakes will be positively related to the chance of a campaign being fraudulent. This hypothesis is supported by the data. The spelling error has a strong, significant positive relationship with fraud for the tabletop games ( $\beta = .84$ ,  $n = 162$ ,  $p = .005$ ), as well as for the gadgets ( $\beta = 1.38$ ,  $n = 186$ ,  $p < .001$ ).

#### 4.4.1.5 Sentiment score

We hypothesized that the sentiment analysis will be negatively related to the chance of a campaign being fraudulent. This hypothesis is supported by the data. The sentiment score has a strong, significant negative relationship with fraud for both tabletop games ( $\beta = -2.31$ ,  $n = 162$ ,  $p < .001$ ) and gadgets ( $\beta = -1.90$ ,  $n = 186$ ,  $p = .013$ ).

**Table 3. Logistic regression model for tabletop games (n = 162)**

Predictor	$\beta$	SE	z	p-value
(Intercept)	-7.91	2.13	-3.71	< .001
min_reward	0.04	0.02	2.34	.019
duration_days	0.12	0.04	2.86	.004
word_count	-0.002	0.0007	-2.20	.028
spelling_error_pct	0.84	0.30	2.78	.005
sentiment_score	-2.31	0.65	-3.57	< .001

Note:  $\beta$  = Estimate, SE = Standard Error, z = strength of predictor

**Table 4. Logistic regression model for gadgets (n = 186)**

Predictor	$\beta$	SE	z	p-value
(Intercept)	-7.94	1.82	-4.36	< .001
min_reward	0.01	0.004	2.05	.040
duration_days	0.11	0.03	3.49	< .001
word_count	-0.001	0.0006	-1.76	.078
spelling_error_pct	1.38	0.26	5.33	< .001
sentiment_score	-1.90	0.76	-2.50	.013

Note:  $\beta$  = Estimate, SE = Standard Error, z = strength of predictor

## 4.5 ROC AUC curve

The Receiver Operating Characteristic Area Under the Curve (ROC AUC) measures how well the model can tell the difference between a fraudulent and a legitimate project. The value should be between 0 and 1. The closer the value is to 1, the better the model can determine whether a project is fraudulent or not. For the tabletop games, this value equals 0.9355. The category gadgets received a value of 0.9385. This means that the model is very likely to distinguish fraud from non-fraud in both categories. Both ROC curves can be found in Appendix 6.3.

## 5. DISCUSSION

Table 5 summarizes the hypotheses of campaign characteristics associated with fraudulent behaviour in the two categories that were analysed: tabletop games and gadgets. The results show that most of the hypotheses are supported by the data from the logistic regression that was conducted. These findings provide statistical support that the variables tested (min\_reward, duration\_days, word\_count, spelling\_error\_pct, and sentiment\_score) are effective indicators of potential fraud in crowdfunding campaigns.

**Table 5. Hypotheses on fraudulent campaign characteristics in Tabletop Games (n = 162) and Gadgets (n = 186)**

Hypothesis	Category	Supported
H1: Time frame will be positively related to the chance of a campaign being fraudulent.	TG	Yes
	G	Yes
H2: The minimum height of a reward to receive a physical product will be positively related to the chance of a campaign being fraudulent.	TG	Yes
	G	Yes
H3a: The number of words in the description will be negatively related to the chance of a campaign being fraudulent.	TG	Yes
	G	No
H3b: The percentage of spelling mistakes will be positively related to the chance of a campaign being fraudulent.	TG	Yes
	G	Yes
H3c: The sentiment analysis will be negatively related to the chance of a campaign being fraudulent.	TG	Yes
	G	Yes

Note: TG = Tabletop Games, G = Gadgets

The goal of this research was to determine the fraud rates among different reward-based crowdfunding categories. The assumption during this research was that fraud rates may correlate with certain campaign characteristics. The results confirm this assumption and show that characteristics such as reward level, funding duration, and the quality of the description can serve as indicators for possible fraudulent behaviour. The analysis revealed that campaigns within the gadget category were more likely to be marked as potentially fraudulent compared to those in tabletop games. This supports the idea that different campaign types attract different types of creators, backers, and risk factors.

This study proposes a practical fraud detection framework for crowdfunding campaigns that evaluates campaign characteristics to assess fraudulent behaviour. The model includes five variables:



- **Minimum reward:** A higher minimum pledge was associated with a greater likelihood of fraud.
- **Campaign duration:** campaigns with a longer funding duration show a greater likelihood of fraud.
- **Word count:** Shorter campaign descriptions are more likely to be connected to fraud.
- **Spelling error percentage:** Spelling errors are more likely to be found in descriptions of fraudulent campaigns.
- **Sentiment score:** Campaigns with a negative sentiment were more often marked as fraudulent.

For each of these variables, a threshold was determined. When a campaign met at least three out of five of these criteria, it was marked as possibly fraudulent. This simple scoring system produced high predictive accuracy, with ROC AUC scores of 0.9355 for tabletop games and 0.9385 for gadgets, which suggests that the model is effective.

What distinguishes this framework is its ease of use and applicability. This model does not require insider data or subjective user ratings, but relies on publicly available campaign information that can be automatically extracted and analysed. As a result, the model can be used by different stakeholders in the field of crowdfunding. This model enables a proactive approach that helps identify high-risk campaigns before they receive large amounts of funding.

In summary, this study demonstrates that fraudulent crowdfunding campaigns have unique, measurable characteristics that can be detected through a quantitative analysis. It also shows that some crowdfunding categories are more vulnerable to fraud than others. These findings not only offer opportunities for new research but also serve as a basis for the development of helpful tools aimed at improving safety, trust, and transparency in the crowdfunding field.

## 5.1 Conclusion

The primary objective of this study was to gain a better understanding of the occurrence of fraud in different categories within reward-based crowdfunding and to provide backers with an estimation of whether a crowdfunding campaign could be fraudulent. The analysis revealed a clear difference in fraud vulnerabilities between the two categories, tabletop games and gadgets. The category gadgets contains the highest fraud rate, with 28 out of 186 (15.05%) of campaigns that did not reach the market being marked as fraudulent. The category of tabletop games has a lower vulnerability, with only 16 out of 162 (6.17%) being marked as fraudulent. This finding directly answers the main research question, “Which reward-based crowdfunding categories are most vulnerable to fraud?”, and shows that the category of gadgets has the highest vulnerability to fraud. Since the parent categories of tabletop games (games) and gadgets (technology) are among the top three most funded categories, they are attractive targets for scammers. The difference in fraud rates indicates the need for fraud detection and prevention tools that are customized for the specific categories, since different types of crowdfunding campaigns may carry different kinds of fraud risks.

## 5.2 Limitations

When interpreting the results of this research, several limitations should be kept in mind. One of the biggest challenges during the development of the model was the lack of confirmed fraudulent cases. Since Kickstarter does not publicly announce the campaigns that turn out to be fraudulent, no officially verified fraud cases could be used to test the model. This makes it difficult

to label a campaign as fraudulent with 100% accuracy. Another limitation is the number of categories this study focused on. Due to time limitations, we only concentrated on two subcategories: Tabletop games and gadgets. These were chosen based on the fact that their parent categories are among the most popular and highest-funded categories on Kickstarter. Other categories, such as art, fashion, or journalism, might have different fraud patterns for which the thresholds of the variables need to be changed. This means that the model created might not automatically apply to the other categories as well.

During the analysis of the description, we noticed several limitations with the spelling checker. The American-English dictionary was used, since we selected the campaigns based on their American location. When a description is written in British English, the spelling checker marks all British words as wrong, even though the word is technically spelled correctly. An example of this situation is the words “organization” and “organisation”. Also, slang is marked as misspelled since it does not occur in the American dictionary. Often, the name of a product is a non-existent word, which would be marked as wrong. To solve this problem, all words that occur in the title of the campaign are excluded from the spelling checker. However, if a campaign did not mention the name of their product in their title, it would be marked as misspelled when it does occur in the description.

Additionally, during the analysis of the description, we found another limitation related to the sentiment analysis. The sentiment analysis evaluates all words individually and does not look at the context. This means that irony, sarcasm, or nuances are not detected. While the sentiment of the description was an important variable for this research, it could be improved by using an advanced model that is able to detect natural language.

The last limitation is that both datasets, tabletop games and gadgets, do not contain the same number of projects. Although the campaigns for each dataset were selected on a consistent process, the difference in sample size could lead to some minor complications. A smaller sample size will have a lower statistical power than a larger sample size. Also, outliers have a bigger influence on a smaller sample size than on a larger sample size.

## 5.3 Future research

The results from this study can be used as a foundation for future research by exploring additional variables and expanding the scope of this research to more categories of reward-based crowdfunding. Possible new variables could be the detection of the use of AI, either in the description or for images. An AI image generator could be used to create prototypes for products that do not exist. The use of AI makes it easier for scammers to create campaigns that seem legitimate, since they can instruct the AI to generate images or descriptions that avoid the criteria that are used to mark a campaign as fraudulent. The second variable that could be added to this model is engagement with users. This variable could be explored to determine if engagement with users is related to the chance of possible fraud. With user engagement, we mean the level of interaction between the creator of a campaign and its (potential) backers. Data that could be used for this is the number of updates, comments, and FAQ a campaign offers. A high engagement can potentially signal transparency and trust, which are usually associated with legitimate campaigns.

As of now, determining whether a crowdfunding campaign is fraudulent takes two main steps. The first step involves web scraping campaign data by entering the campaign’s URL into the application Octoparse. Step two involves the calculation of missing variables and determining the score of fraud in RStudio. Future research could develop an automated system or tool that

combines both steps into a single process. In the ideal situation, a user would only have to enter the URL of the crowdfunding campaign in this tool, after which the program automatically extracts the necessary data and calculates whether or not the crowdfunding campaign could be fraudulent. This would make the fraud detection model faster, more efficient, and user-friendly.

Future research could also extend the model by providing a fraud score with more precision. For example, a percentage-based scoring system for which the output would be: "This crowdfunding campaign has a XX% chance of being fraudulent. Also, a classification score could be taken into consideration with the scores "Definitely fraud", "Probably fraud", "Probably not fraud", and "Definitely not fraud".

## 5.4 Practical Implications

The findings of this study have several practical implications for different stakeholders in the crowdfunding field. The model can be used by potential backers as a risk assessment tool to evaluate the legitimacy of the crowdfunding campaign before they decide to invest. This model provides more information to the backer and reduces the information asymmetry between the backer and the creator of the crowdfunding campaign. Furthermore, crowdfunding platforms could use the model to pre-screen the campaign before there are published on their platform. If the model marks the campaign as fraudulent, the platform can notify the creator of the campaign that he/she need to improve their campaign page before they are able to publish it. This enables platforms to prevent fraudulent campaigns from being published in the first place. For campaign creators, the model could be used as a form of feedback. When a legitimate campaign is being marked as fraudulent, the creator knows that their campaign page needs to be improved in order to attract more backers.

On the negative side, scammers might use the model to improve their fraudulent campaign as well as to make it look legitimate.

However, this is likely a small risk, since improving a campaign requires time and effort. Scammers tend to seek fast and effortless ways to steal money. This means that the benefits of the model outweigh the risks.

## 5.5 Theoretical implications

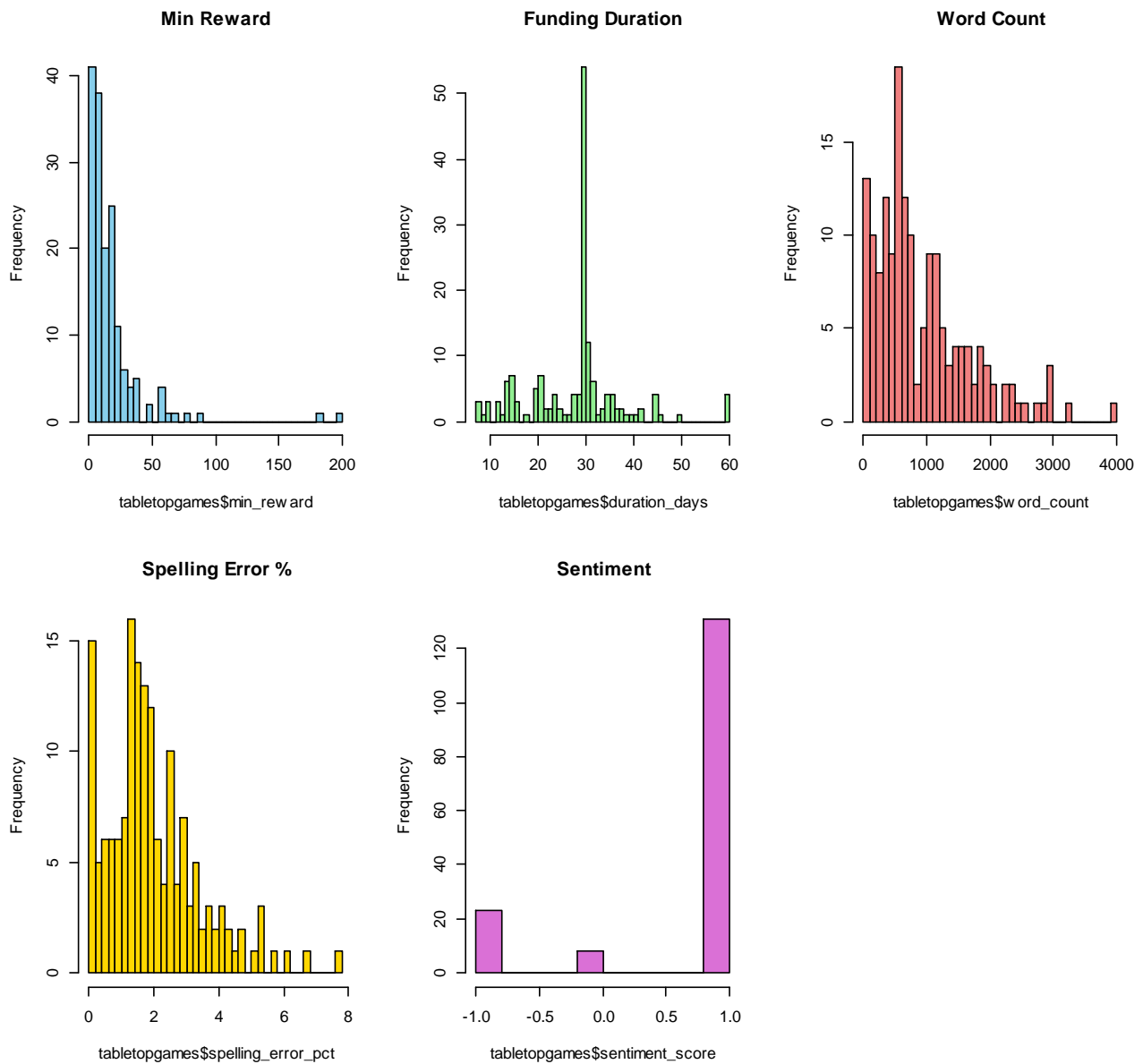
This study contributes to theoretical domains in the fields of fraud detection, crowdfunding, and online trust. Firstly, the results provide support to the Fraud Triangle Theory (FTT), which explains that people commit fraud based on opportunity, pressure, and rationalization. By identifying the campaign characteristics such as unusually high rewards (which could indicate perceived pressure to commit fraud), longer funding duration (which indicates an extended opportunity for fraud) and a higher percentage of spelling errors or a negative sentiment in the description (which are in line with rationalization and lack of professionalism).

Secondly, the findings of this study extend the information asymmetry theory within crowdfunding by showing how reward structures and language indicators can make asymmetry worse. In particular, it seems that fraudulent campaigns take advantage of this information gap by using misleading descriptions or unclear information, which makes it difficult for backers to evaluate the reliability of the project. Therefore, the results indicate that information asymmetry in crowdfunding involves not just the quantity of information offered but also its quality and transparency.

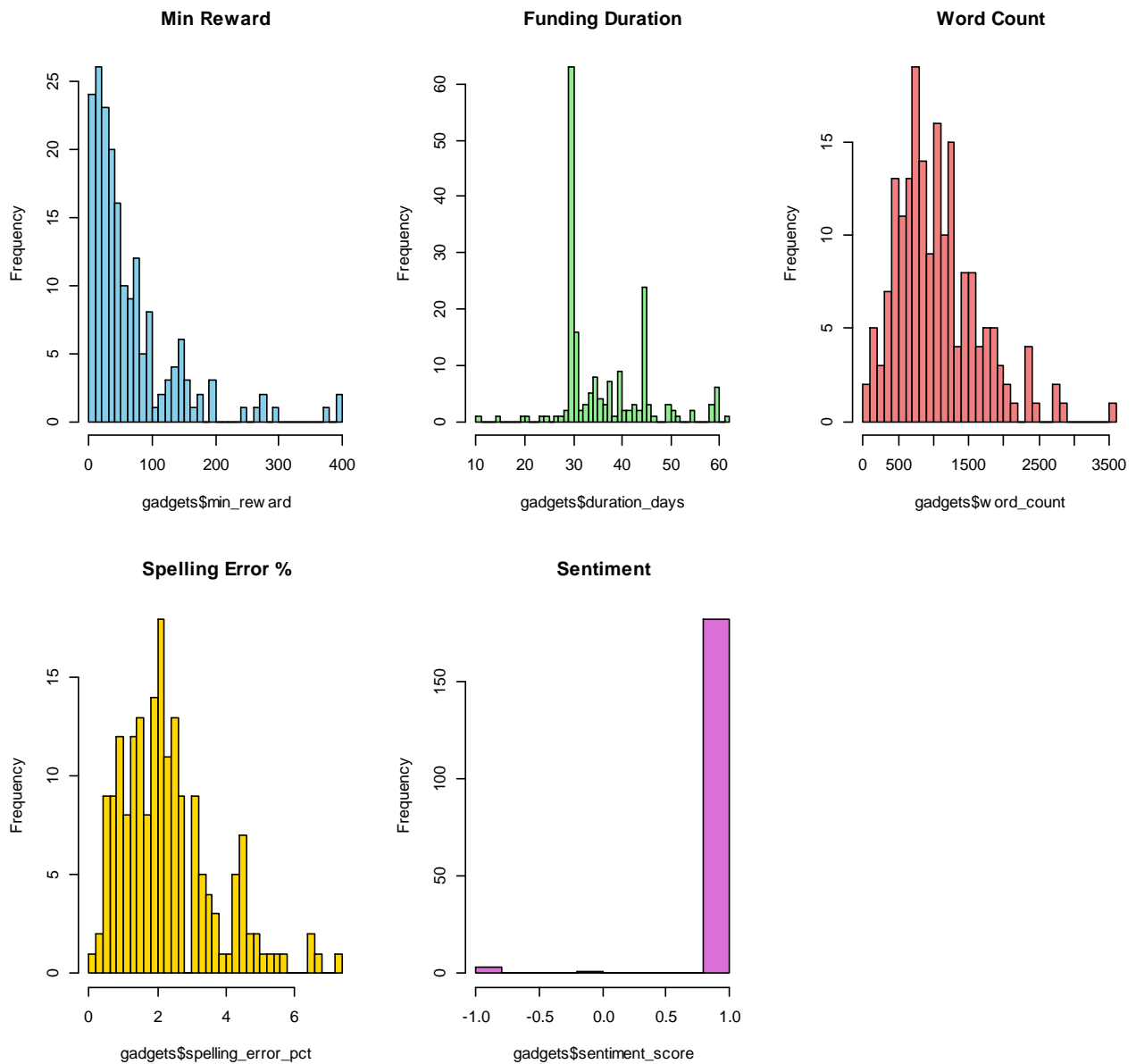
Lastly, the study contributes to crowdfunding literature by showing that fraudulent behaviour is not evenly distributed across all categories. The difference in fraud rates between tabletop games (6.17%) and gadgets (15.05%) suggests that fraud dynamics may vary by category. This supports the idea that certain crowdfunding categories are more attractive for scammers than others.

## 6. APPENDIX

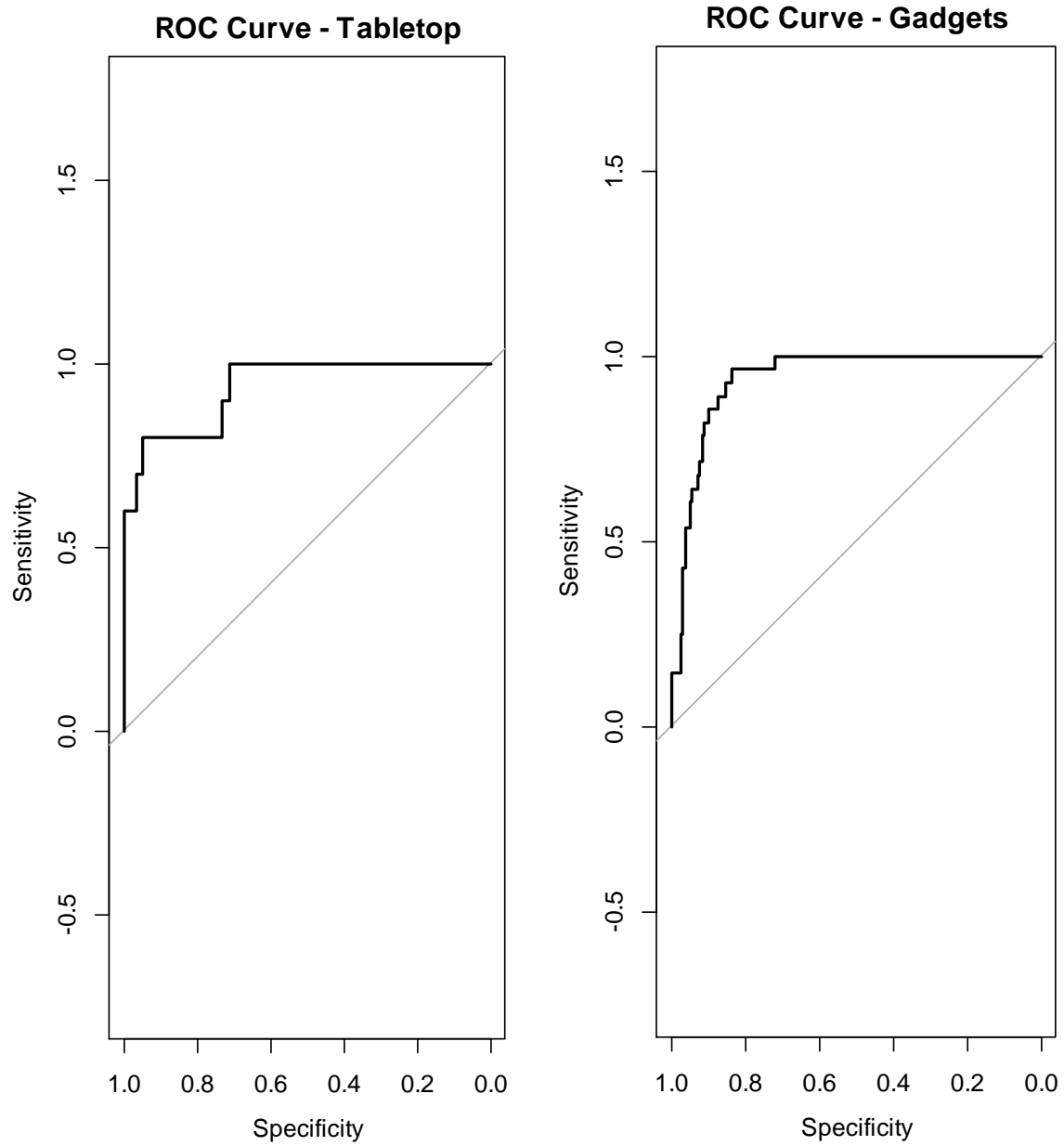
### 6.1 Histograms Tabletop Games



## 6.2 Histograms gadgets



### 6.3 ROC curves



## 7. REFERENCES

- Appio, F. P., Leone, D., Platania, F., & Schiavone, F. (2020). Why are rewards not delivered on time in rewards-based crowdfunding campaigns? An empirical exploration. *Technological Forecasting and Social Change*, 157. <https://doi.org/10.1016/j.techfore.2020.120069>
- Baber, H. (2020). *Blockchain-Based Crowdfunding*.
- Chakraborty, S., & Swinney, R. (2021). Signaling to the crowd: Private quality information and rewards-based crowdfunding. *Manufacturing and Service Operations Management*, 23(1), 155–169. <https://doi.org/10.1287/MSOM.2019.0833>
- Cumming, D., Hornuf, L., Karami, M., & Schweizer, D. (2023). Disentangling Crowdfunding from Fraudfunding. *Journal of Business Ethics*, 182(4), 1103–1128. <https://doi.org/10.1007/s10551-021-04942-w>
- Ellman, M., & Hurkens, S. (2019). Fraud tolerance in optimal crowdfunding. *Economics Letters*, 181, 11–16. <https://doi.org/10.1016/j.econlet.2019.04.015>
- European Union. (n.d.-a). *Peer-to-peer lending*.
- European Union. (n.d.-b). *Reward-based Crowdfunding*. Retrieved March 19, 2025, from [https://single-market-economy.ec.europa.eu/access-finance/guide-crowdfunding/different-types-crowdfunding/rewards-based-crowdfunding\\_en#:~:text=Description,services%20at%20a%20later%20stage](https://single-market-economy.ec.europa.eu/access-finance/guide-crowdfunding/different-types-crowdfunding/rewards-based-crowdfunding_en#:~:text=Description,services%20at%20a%20later%20stage)
- Flor, M., Futagi, Y., Lopez, M., & Mulholland, M. (2015). Patterns of misspellings in L2 and L1 English: a view from the ETS Spelling Corpus. *Bergen Language and Linguistics Studies*, 6(0). <https://doi.org/10.15845/bells.v6i0.811>
- GoFundMe. (n.d.). *GoFundMe Giving Guarantee*. Retrieved April 7, 2025, from <https://www.gofundme.com/c/safety/gofundme-guarantee>
- Hartmann, F., Grottolo, G., Wang, X., & Lunesu, M. I. (2019). *Alternative fundraising: success factors for blockchain-based vs. conventional crowdfunding*.
- Hossain, M., & Creek, S. A. (2021). *Unveiling and Brightening the Dark Side of Crowdfunding*. <https://cmr.berkeley.edu/2021/09/unveiling-and-brightening-the-dark-side-of-crowdfunding/>
- Kassem, R. (2012). *The New Fraud Triangle Model*. <https://www.researchgate.net/publication/256029158>
- Kickstarter. (n.d.). *Kickstarter*. Retrieved March 19, 2025, from [www.kickstarter.com](http://www.kickstarter.com)
- Koch, J.-A., & Siering, M. (2015). *CROWDFUNDING SUCCESS FACTORS: THE CHARACTERISTICS OF SUCCESSFULLY FUNDED PROJECTS ON CROWDFUNDING PLATFORMS*. <http://ssrn.com/abstract=2808424>
- Kumar, K., Vashist, R., & Vashist, P. C. (2023). A Trustful Payment System for Crowdfunding using Blockchain. *2023 International Conference on Artificial Intelligence and Smart Communication, AISC 2023*, 774–780. <https://doi.org/10.1109/AISC56616.2023.10085649>
- Lee, S. H., Shafqat, W., & Kim, H. C. (2022). Backers Beware: Characteristics and Detection of Fraudulent Crowdfunding Campaigns. *Sensors*, 22(19). <https://doi.org/10.3390/s22197677>
- Li, Q., & Qu, J. (2022). Automatic Detection of Fake Crowdfunding Projects. In *INTERNATIONAL SCIENTIFIC JOURNAL OF ENGINEERING AND TECHNOLOGY* (Vol. 7, Issue 2). <https://gearjunkie.com/news/triton-artificial-gills-breathe-underwater>
- Macari, A., & Chun Guo, G. (2021). Perceived violations of reward delivery obligations in reward-based crowdfunding: an integrated theoretical framework. *New England Journal of Entrepreneurship*, 24(1), 43–59. <https://doi.org/10.1108/NEJE-08-2019-0035>
- Machado, M. R., Florina Coita, I., Gómez Teijeiro, L., Wenzlaff, K., Gregoriades, A., Themistocleous, C., van Heeswijk, W., Sinan Bernard, F., Antonio Muñoz, J., Bolesta, K., Osterrieder, J. R., Liu, Y., Dzurovski, A., Stanca, L., Serhan Aydin, N., Rupeika-Apoga, R., Teng, H.-W., Nur Yilmaz, G., Peliova, J., ... Rudnichka bb, st. (2024). *Crowdfunding Fraud Detection: A Systematic Review highlights AI and Blockchain using Topic Modeling*.
- Mollick, E. (2014). The dynamics of crowdfunding: An exploratory study. *Journal of Business Venturing*, 29(1), 1–16. <https://doi.org/10.1016/j.jbusvent.2013.06.005>
- Nguyen, L. T. Q., Hoang, T. G., Do, L. H., Ngo, X. T., Nguyen, P. H. T., Nguyen, G. D. L., & Nguyen, G. N. T. (2021). The role of blockchain technology-based social crowdfunding in advancing social value creation. *Technological Forecasting and Social Change*, 170. <https://doi.org/10.1016/j.techfore.2021.120898>
- Perez, B., MacHado, S., Andrews, J., & Kourtellis, N. (2022). I call BS: Fraud Detection in Crowdfunding Campaigns. *ACM International Conference Proceeding Series*, 1–11. <https://doi.org/10.1145/3501247.3531541>
- Qiu, C. (2013). *Issues in Crowdfunding: theoretical and empirical investigation on Kickstarter*. <http://ssrn.com/abstract=2345872> [Electroniccopyavailableat:http://ssrn.com/abstract=2345872](http://ssrn.com/abstract=2345872)
- Sánchez-Aguayo, M., Urquiza-Aguilar, L., & Estrada-Jiménez, J. (2021). Fraud detection using the fraud triangle theory and data mining techniques: A literature review. In *Computers* (Vol. 10, Issue 10). MDPI. <https://doi.org/10.3390/computers10100121>
- Sarmah, S. S. (2018). Understanding Blockchain Technology. *Computer Science and Engineering*, 8(2), 23–29. <https://doi.org/10.5923/j.computer.20180802.02>
- Smith, T. (2024, May 30). *Crowdfunding: What It Is, How It Works, and Popular Websites*. <https://www.investopedia.com/terms/c/crowdfunding.asp>
- Spence, M. (1973). Job Market Signaling. *The Quarterly Journal of Economics*.

- University Lab Partners. (2020). *5 Most Popular Types of Crowdfunding for Startups*.
- van Teunenbroek, C., & Bekkers, R. (2020). View of Follow the crowd\_ Social information and crowdfunding donations in a large field experiment. *Journal of Behavioral Public Administration*.
- van Teunenbroek, C., Dalla Chiesa, C., & Hesse, L. (2023). The contribution of crowdfunding for philanthropy: A systematic review and framework of donation and reward crowdfunding. *Journal of Philanthropy and Marketing*, 28(3). <https://doi.org/10.1002/nvsm.1791>
- Yacoub, G., Mitra, P., Ratinho, T., & Fatalot, F. (2022). Sustainable entrepreneurs: what drives them to engage in different crowdfunding types? *International Journal of Entrepreneurial Behaviour and Research*, 28(4), 980–1000. <https://doi.org/10.1108/IJEBr-05-2021-0321>
- Yasar, B., Sevilay Yılmaz, I., Hatipoğlu, N., & Salih, A. (2022). Stretching the success in reward-based crowdfunding. *Journal of Business Research*, 152, 205–220. <https://doi.org/10.1016/j.jbusres.2022.07.053>
- Zkik, K., Sebbar, A., Fadi, O., Kamble, S., & Belhadi, A. (2024). Securing blockchain-based crowdfunding platforms: an integrated graph neural networks and machine learning approach. *Electronic Commerce Research*, 24(1), 497–533. <https://doi.org/10.1007/s10660-023-09702-8>