Preventing misuse of discount promotions in e-commerce websites: an application of rule-based systems

G. Vishnu Manohar

Department of Management,
Amrita Vishwa Vidyapeetham,
Amritapuri, Kollam, 690525, India
Email: vishnumanoharg@outlook.com

Biplab Bhattacharjee*

Information Systems and Analytics,
Indian Institute of Management, Shillong,
Meghalaya, 793014, India
Email: biplab.data1@gmail.com
*Corresponding author

Maheshwar Pratap

Department of Management,
Amrita Vishwa Vidyapeetham,
Amritapuri, Kollam, 690525, India
Email: msmpratap@gmail.com

Abstract: E-commerce websites continue to get affected by fraudulent online activities in spite of the substantial efforts made by different stakeholders such as card issuers, banking intermediaries, merchants, and law enforcement agencies. First-time promotional discounts are offered by e-commerce websites for gaining and retaining new and existing customers. However, in several instances, such discounts are abused by fraudsters. Surprisingly, little attempt has been put in the past to detect such abuses. This study is the first attempt in this direction and uses transaction data of an e-commerce company to develop a rule-based detection system. The rules-based system is developed in two-stage processes, generation of facts and rules, respectively; and it is further validated by experts. An architecture of a rule-based fraud detection system is also proposed. Using rule-based detection system, the company can flag-off the probable abusers, and can subsequently monitor their behaviour and take decisive actions.

Keywords: e-commerce fraud; promotional abuse; fraud detection; preventing misuse; discount promotions; e-commerce website; rules-based systems; online fraud; fraud prevention.

Reference to this paper should be made as follows: Manohar, G.V., Bhattacharjee, B. and Pratap, M. (2021) 'Preventing misuse of discount promotions in e-commerce websites: an application of rule-based systems', *Int. J. Services Operations and Informatics*, Vol. 11, No. 1, pp.54–74.

Biographical notes: G. Vishnu Manohar completed his Master in Business Administration from Amrita School of Business, Amrita Vishwa Vidyapeetham, Amritapuri. Prior to his Master's degree, he has completed his Bachelor's in Engineering in Mechanical Engineering from Mangalore Institute of Technology and Engineering. His research interest lies in marketing, data analytics and operations research.

Biplab Bhattacharjee, PhD, is an Assistant Professor in Information Systems and Analytics Area in Indian Institute of Management, Shillong. He holds a PhD. in Systems and Business Analytics from National Institute of Technology Calicut, and has completed his MSc Engg. by Research and Bachelor of Engineering. His research interests include data sciences, business analytics, financial network analysis, system sciences, digital and web analytics. He has extensively published research papers on data science applied to management and bioinformatics domains in several international journals, such as *PLoS One*, *Journal of King Saud University – Computer and Information Sciences*, *Data*, *Journal of Systems and Information Technology*, *International Journal of Business Information Systems*, *Frontiers in Artificial Intelligence and Application*, and in several conference proceedings.

Maheshwar Pratap is an Assistant Professor in the Department of Management, Amrita Vishwa Vidyapeetham, Amritapuri Campus. He is currently pursuing his PhD from Amrita Vishwa Vidyapeetham, Coimbatore. Prior to joining academic career, he completed his Master's in Business Administration and BSc from Amrita Vishwa Vidyapeetham. His research interests include analytics, econometrics and sociology.

1 Introduction

The e-commerce sector in India is expected to have a market size of $200 billion by 2027 from its current value of $64 billion in 2020 (Keelery, 2020). As the e-commerce industry grows, there is also steady incline in types and frequencies of fraudulent activities committed at various stakeholder levels. Fraudsters are finding innovative ways to beat the system and earn from these activities. A study by J.P. Morgan in 2019 on payment trends in India, found out that businesses are expected to lose 4–5% of their total revenue due to fraudulent activities (JPMorgan, 2020). This report indicates that e-commerce businesses in India might lose a whopping $3.2 billion or more in the year 2020 alone due to these kind of activities. Thus, it is imperative that e-commerce companies build tools that detect and prevent fraudulent transactions by consumers as well as merchants.

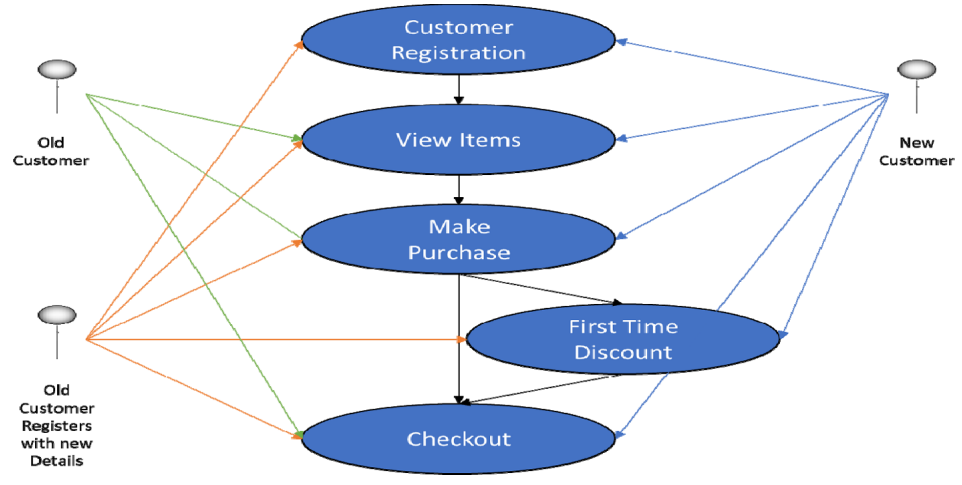
E-commerce companies, along with their different stakeholders such as; card issuers, banking intermediaries, merchants, and law enforcement agencies, have put substantial efforts to curb fraudulent activities. However, as the variety and the frequency of such activities increases, companies are also trying to adopt diverse measures to deal with them. There exist several myriad ways through which e-commerce websites get defrauded. Some of them are chargeback frauds, clean frauds, affiliate frauds, triangulation frauds, reshipping frauds, account takeover frauds, and promotion abuse frauds. In each of these type of frauds, fraudsters devise unique techniques and ways to find loopholes in the system and make profits from those gaps. In the extant literature, several methods have been suggested by various researchers to deal with the different

fraud types across varied industries. Some of the computational approaches used by past researchers in fraud detections, in general, includes data mining (Aleskerov et al., 1997), artificial intelligence (Wheeler and Aitken, 2000), machine learning (Kokkinaki, 1997), genetic programming (Assis et al., 2014), reinforcement learning (El Bouchti et al., 2017), transformed-domain-based method (Saia and Carta, 2019), and combined criteria method (Huang et al., 2017). In the e-commerce sector also, many such methods have been deployed to detect different types of fraudulent behaviours, and relative success has been duly achieved.

Among the various types of e-commerce frauds that are known today, a less reviewed and scrutinised fraud is the promotion abuse fraud. Many e-commerce merchants offer benefits to account holders in their e-commerce portals in terms of promo codes or first-time discounts. This type of discounts has altered the incentivisation strategies of e-commerce companies. For instance, several e-commerce companies offer discounts in the first purchase or alternatively provide free gifts (also referred to as gift cards) with purchases. Such discounts find their presence in all e-commerce businesses such as food ordering, apparels, gadgets, hotel bookings, travel bookings, and other sectors. Behind such discounts, the intention is to attract and bring new customers into the business. Also, such discounts help in signing-up of new users and referring of the e-commerce sites or apps by existing users to their friends and families (Gunasekaran, 2020). It is generally assumed that such types of coupons or promo codes transform new users into the category of regular customers. Companies generally think that such types of discounts are indicative of 'order legitimacy' and hence much attention is not devoted towards misuse of such discounts by fraudsters (Gunasekaran, 2020). However, there are rampant cases of promotion abuses in several e-commerce companies worldwide. This type of abuses may involve multiple usages of coupons by the same individual or creation of many fake accounts by the same person.

The current study is focussed on the first-time discount abuse in the e-commerce sector. Figure 1 illustrates a typical scenario of misuse of a first-time discount offer on an e-commerce website. The figure illustrates the promotional abuse using three scenarios. In the first case, a new customer visits the e-commerce website and goes through the following sequential processes. The customer registers or signs-up at the website, and post-registration, the customer views the items to be bought. In the next step, he attempts to make an order for purchase, and thereby, he becomes eligible for 'first-time customer discount'. Subsequently, he pays the amount and checks-out of the portal. In the second case, an old (or existing) customer need not go through the customer registration process as followed in case 1, since his/her details are pre-recorded in the company transactional database. So, an old customer directly views the items, and subsequently pays and purchases it. In this case, the customer does not become eligible for a first-time discount. In the third case wherein promotional abuse is attempted, an old customer poses as a new customer by registering at the website with new user details and proceeds through the sequence of activities as in case 1. Since, the system becomes unable to identify the customer as an existing one using the recorded database, the first-time discount gets applied to him. This schema is used by the fraudsters for misusing first-time promotional discount offers by duplicating their user details.

Figure 1 A typical scenario of misuse of a first-time discount offer in e-commerce (see online version for colours)



Source: Adapted from Fakhroutdinov (2020)

In this study, we attempt to propose a fraud detection system for first-time promotional discount abusers. The study uses real historical transactional data of an e-commerce company for building the detection system. A rule-based approach has been proposed in this study, and the consequential steps that the e-commerce company can perform are also discussed. An architecture of the rule-based system is also described. Traditionally, rule-based engines are considered as a first step for designing a decision expert system for a new case. A machine learning (ML) approach has not been implemented here because of two reasons. First, the data provided in the study were not labelled, and with the raw attributes in hand, nothing consequential learning could be done on a machine learning platform. Second, the datasets provided for building the model was relatively smaller in size; hence, a rule-based modelling was preferred than a ML model. Also, the final-users of the detection system desired more interpretable rules from the dataset than a complex ML model.

For building the rule-based engine, the dataset used was obtained from an e-commerce company that uses Shopify's cloud-based solution. The dataset was received in an anonymised condition for confidentiality. The dataset consisted of 1000 transactions by the customers, with each transaction having 65 number of attributes. The dataset is filtered and split into new and existing customer entries. The various attributes in the dataset are studied, and the insignificant attributes in relation to promotional abuse are removed prior to building the rule-based engine. From the residual set of attributes, a set of facts and rules are generated to identify possible fraudulent transactions.

The rest of the paper proceeds as follows: Section 2 consists of the literature review, and Section 3 provides both the research objectives and the assumptions considered in the model. In Section 4, the methodology adopted is detailed, and Section 5 explains the results and discussions. Section 6 gives the managerial implications, limitations, and the future scope of the study.

2 Literature review

2.1 Frauds in e-businesses

Fraud is a deceptive criminal act aimed at making economic or personal gains. Fraud is a blanket term that encompasses all the diverse means that human imagination can conceive and that are used by persons to gain an undue advantage over another individual or organisation either through false suggestions or by suppressing the truth (Rezaee, 2002). There are several types of fraud of electronic nature such as, credit card, telecommunication, computer intrusion, bankruptcy, counterfeit, application, and behavioural frauds (Chaudhary et al., 2012). All these fraud types are briefly discussed below. In the extant literature, the credit card frauds are normally classified into two categories, frauds committed in online and offline activities, respectively. The former one is committed by fraudsters in the absence of card-holder and during shopping via telephonic or web mediums. The later one is committed in cases where the credit cards are stolen by fraudsters and are further misused. The next type of fraud, i.e. telecommunications fraud, has also been grouped under two classes, namely superimposed frauds and subscription frauds. The former one occurs when a service is used by a fraudster without having the prior essential authorisation. The later one occurs in cases where a service is subscribed with false details, and there is no payment intention (Kou et al., 2004). The third type of fraud, i.e. intrusions into information systems can take many forms such as, swiftly propagating a virus or a worm, not allowing services by flooding resources, or obtaining privileges of root users with an intention to do malicious activities (Ye et al., 2003). The fourth type of fraud, i.e. the bankruptcy fraud, as the name implies, involves the credit card usage when the condition of the user is in bankruptcy or insolvency states. In simple terms, it means that credit card users do purchases with the full knowledge that they would be unable to repay the amount in the future. In such circumstances, banks will be in no position to recover the debt and will have to cover the losses by themselves (Delamaire et al., 2009). The fifth type of fraud is counterfeit fraud which occurs during remote usage of credit cards. These kinds of frauds happen in cases wherein the only details necessary for credit card usage are card numbers and card verification value (CVV), respectively. (Chaudhary et al., 2012). The sixth type of fraud, i.e., application fraud, occurs when someone applies for a credit card by impersonation. Credit applications are forms in web-based or paper-based formats, and such applications are filled-in by prospective customers to avail of different types of loans. In credit application frauds, there is theft of real identities, and synthetic identities are created by fraudsters (Phua et al., 2010). Another type of fraud, called behavioural fraud happens in cases where fraudulent ways are adopted to obtain the details of legitimate card-holders and purchases and orders are subsequently made (Chaudhary et al., 2012).

2.2 Frauds in e-commerce

In the context of the e-commerce sector, there are several other diverse ways through which companies are defrauded. Some of them are chargeback, clean, affiliate, triangulation, reshipping, account takeover, and promotion abuse frauds. Each of these fraud types is discussed in brief below. When a legitimate account holder abuses the e-commerce claim system for the purpose of some financial gains, such kinds of abuses

are collectively referred to as chargeback types of frauds. There are different ways this crime can be committed. A customer may make a fraudulent claim on the grounds that they have not received the ordered goods, or they can also assert that all the ordered goods have not been received (Amasiatu and Shah, 2014). A clean fraud happens when a fraudster uses a stolen card to make a purchase. Fraudsters modify their transactions in such a way that detection systems are avoided (Rajeshwari and Babu, 2016). In the case of affiliate fraud, the fraudster generates traffic and signup statistics to glean more money from an affiliate program. This process could either be automated or it can also be executed by using real people to sign up at merchants' websites using fake accounts (Rajeshwari and Babu, 2016). The triangulation fraud, as the name suggests, has three steps. First, fraudsters establish a dummy store and collect customer details, including credit card information. Then, the collected data gets utilised to make purchases, which are shipped to the card owners. Finally, the same details are used by the fraudster to make further purchases for themselves (Wang et al., 2006). In the reshipping fraud, fraudsters buy high-value goods using stolen credit cards and use gullible individuals to collect and forward the shipments on behalf of the fraudsters. Once the goods are obtained by the fraudsters, they sell them for cash on the black market. Over the last few years, reshipping fraud has become one of the key strategies to monetise stolen credit cards (Hao et al., 2015). Account takeover fraud is a kind of fraud wherein a fraudster gains unauthorised access to the account or they may even get complete control of the victims' account (Tao et al., 2018).

2.3 Fraud detection methods in e-commerce

As frauds in e-commerce increases in types and frequencies, companies and academic researchers are also exploring different methods for the detection and prevention of such frauds. Several studies have attempted to work on fraud detection problems in diverse type of e-commerce industries. These studies have focussed on multiple types of e-commerce frauds and have proposed different solutions using a wide range of computational methods. Some of these studies are discussed below. The study by Lek et al. (2001) discusses the building of a prototype based on data mining concepts for fraud-pattern detections and identifications of irregularities in e-commerce transactions. In this study, the authors developed a prototype using the C4.5 algorithm. The study by Shaji and Panchal (2017) discusses an architecture for adaptive mobile learning (ANFIS) model for detection of fraudulent transactions in e-commerce. The study by Carta et al. (2019) used a Prudential Multiple Consensus model for fraud detection in credit card transactions in the e-commerce industry. The study by Caldeira et al. (2014) discusses machine learning models for classifying fraudulent activities in credit card operations performed on web payment gateways. In this study, the models were built using Bayesian networks, logistic regression, neural networks, and random forest algorithms. Many more studies have attempted to build models for fraud detection in credit card transactions in e-commerce space using methods such as, hidden Markov models (HMM), artificial neural networks, random forest, and CART based random forest, Markov decision process, and deep neural networks (Kundu et al., 2009; Lebichot et al., 2019; Mead et al., 2018; Porwal and Mukund, 2019; Srivastava et al., 2008; Tao et al., 2018; Xuan et al., 2018).

The studies by Tao et al. (2018) and Shaji and Panchal (2017) has proposed fraud detection models on account takeover frauds in the e-commerce industry. These studies

used methods such as selective graph attention, long short term memory (LSTM), sequence tagging, adaptive neuro-fuzzy approach, K-Nearest Neighbour, random forest, and isolation forest. The study by Zhao et al. (2016) discusses reasoning-based approaches for detecting collusive fraudulent transactions in e-commerce. The study used an extension of the Classical Dempster–Shafer (DS) uncertainty reasoning model. The study by Polman and Spruit (2013) has worked on fraud detection in post-payment orders in the e-commerce industry. Polman and Spruit (2013) used an integrating model by employing both expert domain knowledge and data mining techniques. The study by Lima and Pereira (2016) has worked on fraud detection models for e-payments in the e-commerce sector. Lima and Pereira (2016) used feature selection approaches for fraud detection. The feature selection in this work was implemented by employing Bayesian networks, logistic regression and decision trees. The study by Quah and Sriganesh (2008) has worked on a detection approach for triangulation fraud. This study used self-organising maps (SOM) for their proposed approach.

Apart from all these techniques, the rule-based engine has also been deployed for fraud detection in several scenarios. The study by Leonard (1995) presented a rule-based expert system which helped to alert banks during the fraudulent usage of credit cards by identifying suspicious activities in authorisation processes. The expert system allowed for analysis of transactions multiple times a day. The study by Fawcett and Provost (1997) used a rule learning program to derive insights from a customer transactional database and identified key behavioural indicators of fraudulent transactions. The authors (Fawcett and Provost, 1997) also used these generated indicators for the purpose of the creation of a set of monitors, which were further deployed in profiling customers having legitimate behaviour and the ones showing deviations, respectively. The study by Rosset et al. (1999) presented an approach for churn management using the rule-based detection model. The model developed in this study allows the operator to predict the churners ranked by their prediction scores. This study identified unique features of rule-discovery for fraud detection in telecommunications.

From the above review of the literature, it is evident that there has been little effort on promotional abuse detections. E-commerce businesses traditionally think of promotional discounts as a way of incentivising sales, and these companies do not give much attention to misuse of such discounts. However, cumulatively a large number of such abuses lead to substantial revenue loss for the company, which would have otherwise been deployed productively in some useful alternative activities. E-commerce companies traditionally spend a large amount on marketing budgets to attract new customers and retain old ones. Promotional discounts form a big chunk in such budgets, and such incentivising schemes leads to higher cash burn rate and mounting losses for these companies. Thus, any attempt to decrease the cash spend on such discounts without impacting new customer addition is always an useful activity. The minimisation of promotional abuses by detection and further decisive actions can, in a more substantial way reduce this expenditure. Also, there are widespread cases of such abuses in multiple e-commerce companies dealing in different sectors such as retail, fashion, grocery, home appliances, books, travel, lodging and other many more businesses. Hence, it is a worthwhile attempt to develop detection systems for preventing such abuses. The current study is a modest attempt to fill this gap in the literature. The current study attempts to develop a rule-based engine to flag-off transactions that are likely to misuse the first-time discount promotions.

3 Research objectives and assumptions

The detection of promotional abusers is a binary classification problem and is based on multi-dimensional attributes. There are a large number of varied attributes that are captured during one single order transaction by a customer. These attributes range from the ones which are fed by a customer during registration and purchase processes and the ones which are automatically captured by the app. The attributes depict the demographic, transaction and financial information, respectively. Thus, it is challenging exercise to identify the ones which can be indicators of promotional abuse by a single individual. An efficient and robust detection system should use a minimal number of input variables for its function. The primary objective of this study is to propose a detection system using the attribute information for identifying transactions likely to perform promotion abuse of first-time discounts. Under this primary objective, the following sub-objectives are attempted:

- to identify attributes in the transaction dataset which is more likely to indicate masking of customer identity
- to generate production rules from the identified attributes in the dataset
- to propose an architecture of the promotional abuse detection system.

The following assumptions have been taken into consideration while building this model:

- the distribution of values of attributes in dataset studied is similar to the ones in production data
- there will be certain attributes which an individual cannot duplicate/multiply several times
- fraudsters follow certain behavioural trends while doing any fraudulent transactions.

4 Methodology

4.1 Dataset description

The dataset in the current study belongs to an e-commerce company. The e-commerce company uses Shopify as a technology platform to manage its operations. Shopify is a cloud-based solution which can be used to create and customise an online store (Shopify Developers, 2020). The data was received in an anonymised condition so as to protect confidentiality. The dataset consisted of orders done using the mobile app of the company during 2018–2019 period. The raw dataset consisted of 1000 orders from the e-commerce company. As per Shopify terminology, an order is referred to a fulfilled request of a customer in which purchase of either single or a multiple number of products happen from an e-commerce website or an app (Shopify Developers, 2020). The creation of order happens when the checkout process is completed by a customer. During the creation of the order, the following information is provided by the customer: billing address, telephone/mobile numbers, email address (or addresses), and payment details. Each of the order in the current dataset had associated 65 attributes, which is typically used in Shopify applications.

4.2 Data pre-processing

Each of the transaction in the current dataset was labelled as 'first-time discount' or 'existing customer'. Based on these labels, the dataset was segregated into new and existing customers. The percentage of new customers in the total dataset was 43.40%. The further steps were performed on the new customer dataset. In the initial steps, each attribute's importance was searched and researched upon using the web documentation provided by Shopify API Developer website (Shopify Developers, 2020).

The dataset had 65 attributes, out of which many were insignificant for the problem in hand. The insignificant attributes are filtered out from the new customer dataset. For the purpose of distinguishing promotional abuse cases, six attributes were considered significant.

4.3 Rule-based engines

One can describe a 'rule-based systems' as a basic kind of artificial intelligence (AI) systems, wherein a series of IF-THEN statements are used to arrive at a decision/ conclusion/recommendation (Grosan and Abraham, 2011). A rule-based system for business decision making has to be fed with a certain number of business rules and the consequent task set. Typically, such a system consists of two key components, which are:

- a set of facts
- a set of rules to deal with those facts.

The two components are discussed below:

1 *A set of facts*: It is also called as the knowledge base. They are basically a combination of certain information. For e.g., CIBIL score and a condition such as 'less than five hundred' (Grosan and Abraham, 2011).

2 *A set of rules*: It is also called as the rules-engine. They form the rules that establish the relationships among two conditional statements, 'IF' and 'THEN'. Consider, for instance, a rule can be stated as, "IF a loan applicant has a CIBIL score between 300 and 500. THEN application must be rejected" (Grosan and Abraham, 2011).

4.4 Generating a set of facts and a set of rules

The first step in the generation of rules-based system is to generate a set of facts, also called a knowledge base. In this study, from the attributes given in Table 1, all possible combinations of data values are identified. For instance, *app_id=580111*.

From the set of facts, rules are constructed. Rules in this study are constructed, taking both single attributes and multiple attributes into consideration. It is assumed that any rules that can identify duplicate entries amongst values in a given attribute are qualified to identify attempts to misuse the system for getting discounts. If for multiple numbers of attributes, the same value for numerous transactions is noticed, those particular attributes are identified. Based on these criteria, rules are listed.

Table 1 List of attributes filtered out before generating the set of facts

S. No.	*Attribute names*	*Reason for filtering out the attributes*
1	_sdc_batched_at,_sdc_extracted_at,_sdc_received_at,_sdc_sequence,_sdc_table_version,admin_graphql_	These are identifiers of the data warehouse from where the data is extracted. These identifiers do not have any relevance for the detection of promotional abuse since they are related to the data warehouse of the e-commerce company.
2	api_id	This is the identifier for the ShopifyAPI. This identifier doesn't have any relevance for the detection of promotional abuse as it only identifies the app that the customer is using in his handheld devices.
2	checkout_id	This a randomly generated identifier for checkout events in an e-commerce transaction. This identifier does not have any relevance for the detection of promotional abuse as it changes for every transaction which completed with checkout.
3	total_discounts, total_discounts_set-presentment_money_amount, total_discounts_set_shop_money_amount	These are numerical values of discount figures that have been given/fixed for a particular order. The discount values does not have any relevance for the detection of promotional abuse since these values are prefixed the company.
4	customer__orders_count, customer__total_spent, subtotal_price, subtotal_price_set__presentment_money__amount, subtotal_price_set__shop_money__amount, total_line_items_price, total_line_items_price_set__presentment_money__amount, total_line_items_price_set__shop_money__amount, total_price, total_price_set__presentment_money__amount, total_price_set__shop_money__amount, total_price_usd, total_shipping_price_set__presentment_money__amount, total_shipping_price_set__shop_money__amount, total_tax, total_tax_set__presentment_money__amount, total_tax_set__shop_money__amount, total_tip_received	These values correspond to the financial details of the order, i.e., about number of orders given, amount spent, price, all in shop currency. This values does not have any relevance for the detection of promotional abuse since it indicates the pricing details of the order.
5	total_weight	This is the summation of weights in grams of all the line-items. This value doesn't have any relevance for the detection of promotional abuse as it refers to only the summed weights of items that are ordered.
6	total_tax, total_tax_set_presentment_amount	These values refer to the total tax that is applicable on order made. The tax here is computed both in presentment and shop currencies. These values do not have any relevance for the detection of promotional abuse as this are taxes that are prefixed by the government regulations.
7	billing_address__country	This gives country's name where the billing address is located. As all orders in the current dataset are from the same country, thus this attribute is irrelevant for the detection of promotional abuse.

Table 1 List of attributes filtered out before generating the set of facts (continued)

S. No.	*Attribute names*	*Reason for filtering out the attributes*
8	billing_address__province, billing_address__province_code	This attributes gives the identifier or the name of the region (province, state, prefecture, …) of the address used in billing. In the current dataset, we have four providences listed. This attribute is irrelevant for the detection of promotional abuse as this depict only the location profile of the customer giving the order.
9	buyer_accepts_marketing	This attribute gives an indication of whether there is a consent given by the customer for sending email updates. This attribute is irrelevant for the detection of promotional abuse as whether consent is received or not does not any way to relate to such abuses.
10	cart_token, checkout_id	These are identifiers associated with the order. These attributes are irrelevant for the detection of promotional abuse as they are unique for each customer order.
11	checkout_token	It manages a customer's given cart as it transitions into a paid checkout. This attribute is irrelevant for the detection of promotional abuse.
12	closed_at	This attribute represents the time and date when the closing of the order was done. This is represented in ISO 8601 format. The time of closing an order has no relevance for the detection of promotional abuse.
13	created_at	This attribute represents the auto-generated time and the date when the creation of the order was done in Shopify. This is represented in ISO 8601 format. The value for this property cannot be changed, thus it is irrelevant for the detection of promotional abuse.
14	taxes_included	This attribute gives an indication of whether the taxes were included in the order subtotal. This attribute is irrelevant for the detection of promotional abuse as this are taxes that are prefixed by the government regulations.
15	updated_at, cancelled_at, cancel_reason	These attributes indicate when an order was updated, when it was updated, and, the reason for cancellation, respectively. These attributes are irrelevant for the detection of promotional abuse.
16	processing_method	This attribute indicates how the payment was processed. It has six valid values. This attribute is irrelevant for the detection of promotional abuse.
17	payment_details__cvv_result_code, presentment_currency	The first attribute indicates whether there was a correct entry of Card Security Code by the customer. The second attribute indicates the currency in which the prices were presented to the customer. These attributes are irrelevant for the detection of promotional abuse.

Table 1 List of attributes filtered out before generating the set of facts (continued)

S. No.	*Attribute names*	*Reason for filtering out the attributes*
18	number, order_number, order_status_url	These attributes represent the order's position in the shops, the count of orders, and the URL address that points towards the webpage containing the order status. These attributes are irrelevant for the detection of promotional abuse.
19	Gateway	There are four payment gateways in this dataset, namely manual, paypal, shopify, and stripe. The type of payment gateway that is used in a transaction has little relevance for the promotional discount detection.
20	fulfillment_status	This attribute has four values, namely shipped, partial, unshipped, and unfulfilled. The status of fulfilment of the shipment doesn't have any relevance in promotional abuse detection.
21	financial_status	There are three options in this attribute, namely paid, partially refunded and refunded. The status of customer payment for the e-commerce order has no substantial relevance to detection of promotional abuse.
22	customer__currency	This attribute indicates the three-letter code for the currency in which they paid for their last order. This attribute is irrelevant for the detection of promotional abuse.
23	customer__created_at	This attribute indicates the timestamps and the dates when the creation of the customer entry were done. This attribute is irrelevant for the detection of promotional abuse.
24	customer__admin_graphql_api_id	This attribute is an identifier used during the migration of the database from the REST Admin API to the GraphQL Admin API. These identifiers don't have any relevance for the detection of promotional abuse since they are related to information system flow of the e-commerce company.
25	customer__accepts_marketing, buyer_accepts_marketing	There are two options in these attributes, true and false. The condition, whether the customer or the buyer accepts marketing has no bearing on promotional abuse.

5 Results and discussions

5.1 Exploratory analysis of the attributes

All the attributes in the new customer dataset are examined for their relevance in the detection of promotional abuse cases. On examining each of these attributes, we obtain a set of attributes which does not have any relevance in fraud detection. Those set of

attributes are filtered out from the dataset prior to making a set of facts. Table 1 provides a list of attributes that have been filtered out. The definition of each of the attributes provided in this table is obtained from Shopify API developer website (Shopify Developers, 2020).

Once the irrelevant attributes (59 attributes) for the transaction dataset are filtered out, the remaining attributes are examined in the further steps for fact generation. Fact generation, in this case, is done on a principle that if an old customer attempts to show himself as a new customer than some part of the data collected from the customer in earlier transactions would be matching with the data collected in the new entry. Thus, the values recorded in each of the remaining attributes are examined carefully, and checked for repeatability in a different set of customer transactions. Repetition of values is an indication of transaction done by individuals having similar characteristics and to some extent, the same individuals. This condition is used as criterion for examining all remaining attributes. From this assessment, six attributes were considered for rule generation. Table 2 provides a description of the six attributes that were considered in this study for rule generation.

Table 2 Significant attributes identified for rules generation

S. No.	*Attribute name*	*Attribute description*	*Reason for considering the attribute*
1	App id	This is the id of the app which created the order. This is akin to the version number that several applications have.	For any existing customer, the app id will be captured in the first transaction, so it can be detected in the subsequent transaction.
2	Billing address name	This gives the complete address of the individual who is linked to transaction's payment method.	A customer feasibly cannot have many billing addresses.
3	Browser IP	The browser IP address that customer used while making the order placement.	A customer will mostly use the same internet connection, having the same IP address for placing an order.
4	Customer default address name	This gives the full name of the default customer.	A customer's default address name cannot be different.
5	Payment details credit card number	The credit card number used for completing the purchase.	A customer can have only limited credit cards, and normally people don't share their credit card details with others.
6	Tags	Tags attached to an order. These are short descriptions, used commonly for searching and filtering.	The tags indicate whether the customer is an existing user or a new user. This is the most relevant attribute as it has been employed sub-setting new customers data from the complete dataset.

5.2 Production rules identified

The final production rules have been identified from six attributes. The production rules identified are from transactions of new users only. The six attributes are abbreviated below.

Consider,

CCN1 = Credit card number of old entries

CCN2 = Credit card number of the new entry

BAN1 = Billing address name of old entries

BAN2 = Billing address name of the new entry

CDAN1 = Customer default address name of old entries

CDAN2 = Customer default address name of old entry

T1 = New Customer First-time transaction

FTDPM = First-time Discount Promotional Abuse.

The following rules have been identified:

R1: IF CCN2 = CCN1, THEN FTDPM = True

R2: IF BAN2 = BAN1, THEN FTDPM = True

R3: IF BAN2 = CDAN1, THEN FTDPM = True.

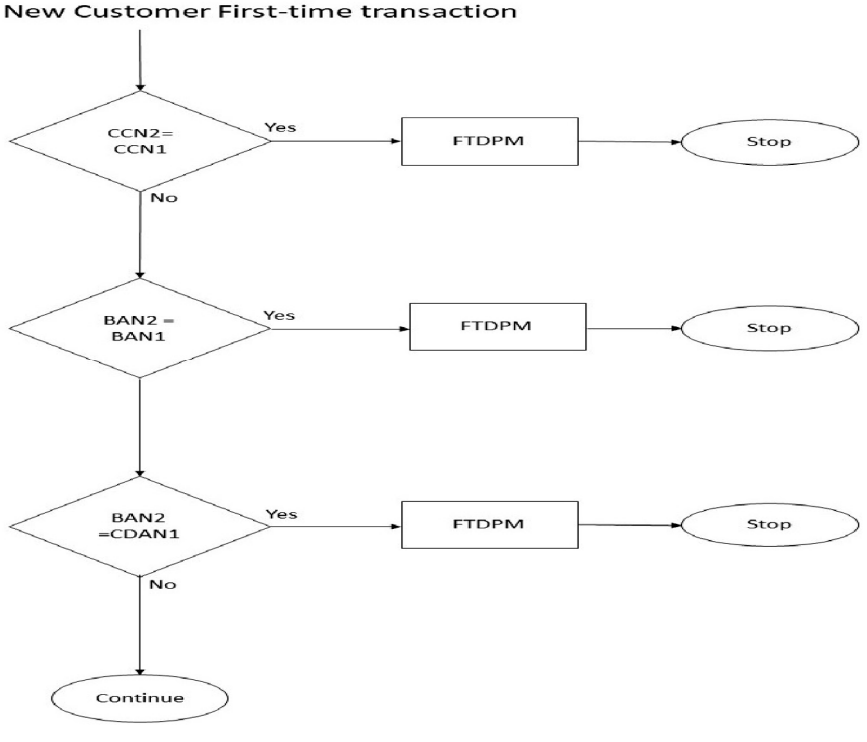
The production rules generated above were further verified by subject matter experts. In a typical implementation of a rule-based system, the following steps are executed (Jones, 2005): In the first step, the working memory and the rules-set are initialised. In the second step, the rule files are parsed. In the third step, the rule matching is performed. There lie two scenarios after that, one when rules are matched, and the second, when the rules are not matched. In the first scenario, once the rules are matched, the consequential steps are performed and then the operation loops back to the next iteration, wherein the rules matching is performed for the next set of data. In the second scenario, if the rules are not matching the operations loops back to the previous step of rules for next set of data.

The functioning of the proposed rules-based engine for promotional abuse detection is illustrated as a flowchart in Figure 2. In this illustration, one can observe that once any transaction happens, and the customer in the transaction claims to be a ‘new customer’, the engine proceeds to match each of the production rules stored in the rules database. In step one, the first rule is applied to new customer entries to verify whether there exists a match of entries with the recorded values in the existing database. If a match of entries is observed, a flag is issued – first time discount abuse. If for a given rule, a suitable match with old entries is not observed, the flow proceeds to the next rule, wherein the data is verified again for rule matching. This continues until:

- a flag has been raised by the rules-engine, where a new customer is flagged as first-time discount abuse
- all the rules in the rules database have been exhausted.

If all the rules in the rules database have been exhausted and no flag issued, then the customer is deemed as a genuine customer, and the first-time promotional discount is applicable to them. If a flag is issued by the rules-based engine, the customer is supposed to be probably promotional abuse case, and his further behaviour would be tracked and scrutinised by the transaction risk management team of the e-commerce firm.

Figure 2 Flowchart depicting the usage of the production rules in the proposed rules-based engine



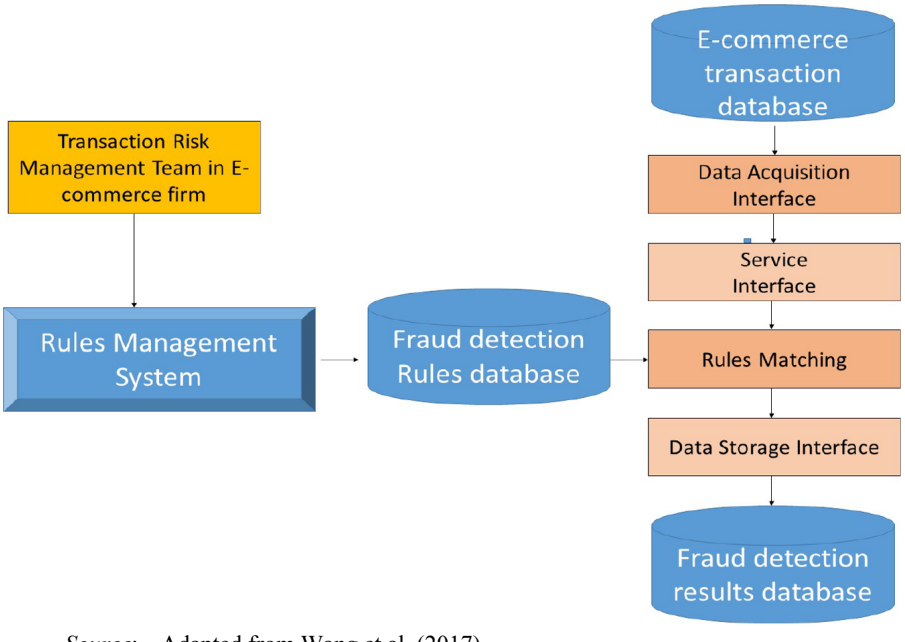
5.3 Proposed architecture of the promotional abuse detection system

Figure 3 provides a proposed architecture for the promotional abuse detection system. The study by Wang et al. (2017) has proposed an architecture for fraud detection systems using rule-based engines. We adapted the architecture of this study with the incorporation of our results.

Majority of the e-commerce companies today has taken recurrent fraudulent activities very seriously, and these organisations have established in-house 'transaction risk management teams' for handling such cases. The rules-based engine can be suitable be deployed by personnel of such teams for promotional abuse detection and subsequent human interventions in the form of tracking and scrutiny. The proposed architecture of the rules-based engine in Figure 3 can perform the following functions: data acquisition for new customers, detection-data storage interface, service interface, rules management, maintaining a database containing rules, and performing matching-operation for the rules. The proposed framework shown in Figure 3 has the following components:

- *Interface for data acquisition and storage*: There are two data interfaces in this proposed architecture, one for data-acquisition and the other for data-storage. These two performs the following functions: i) acquisition of customer data from e-commerce transaction database/data warehouse, and ii) storage of the results from rules-matching exercises to the 'fraud detection results database'. The data storage exercise occurs when an individual first-time signs-up for the e-commerce app/website, and also during every subsequent transaction. The data of rules-matching exercises are saved in every instance when rules engines are triggered off.
- *Service interface*: Through the service interface, the platform triggers the rules engine, which will, in turn, verify historical records of customers.
- *Rules management*: The rules management system connects to the 'fraud detection rules database' for performing its functionality. This system performs the following functions: establishing, modifying, verifying, updating and deleting rules.
- *Fraud detection rules database*: This is the principal component of the framework. It is a stacking of the rule files. It is maintained by rules management.
- *Rules matching component*: This component applies the rules from the 'rules files' stored in the fraud detection rules database. The purpose of this operation is to determine how exactly a new record (of a new customer) matches with existing records of a customer in the database/data warehouse. Then, it flags a new customer as a genuine new customer or a promotional abuse case.

Figure 3 Proposed architecture of the promotional abuse detection system (see online version for colours)



Source: Adapted from Wang et al. (2017)

6 Conclusions

6.1 Managerial implications of the study

E-commerce retailers face a challenging task in preventing frauds and finding an effective response to such attempts by fraudsters. The key advantage in framing a rule-based engine and using it by end-users, i.e. transaction risk management teams in e-commerce firms is that the rules generated are easily interpretable and managers can use their experience and gut feeling along with the outcome of the rules-based engine to make a judicious decision. The rules-based engine proposed can be deployed by the e-commerce company to flag off the transactions and subsequently for referring for human interventions. Using the proposed system, one can assess in real-time each of the transactions, and can further distinguish them as 'genuine' or "promotional abuse" classes. In a real-time implementation, this method can automatically block abusers of first-time discounts from performing any further transactions, once those individuals are 'flagged' as a risky category. Implementation of this method can as well highlight the 'real' users in such a way that there is no loss of genuine customers to the business. Thus, many attempts of promotional abuses can be prevented. In addition to using this detection system, clauses can also be added in the terms and conditions of the discount promotional offers. Clauses stating that any violation will be resulting in blocking existing accounts will do a great purpose. For several e-commerce merchants who are uncomfortable or reluctant in blocking account creation, can take an alternative step like monitoring those accounts which are flagged off and study their behaviour using analytics platform. If any further suspicious behaviour evolves out from such flagged account, then subsequent measures can be taken by the company. These measures will help in a long way in countering such promotional abuses, and reduce the risk of fraudsters beating the system. Promotional discounts come from marketing budgets of e-commerce companies, and in this rapid cut-throat competitions among different service provides, the budgetary amount spend of such activities can be judiciously used once such fraud-abuses can be minimised to a certain extent. As new fraud detection systems are being implemented by e-commerce companies, fraudsters are also becoming very smart to escape such detection systems, however, a system in place can be more effective strategy than status-quo.

6.2 Limitations of the study

The first limitation of the study is that the rules extracted are domain-specific and business-specific. The same rules may or may not hold true for different e-commerce sectors or businesses.

The second limitation of the study is that the dataset provided to the researchers were not labelled as fraud and non-fraud entries. Hence in the absence of labelled data, the current production rules were verified by only subject matter experts.

Also, in the absence of labelled data, the work could not be transformed into a supervised machine learning problem. The model may be further enhanced once labelled data is available. A fuzzy logic approach can also be implemented once labelled data is made available.

Another aspect that can be considered while making rules is the actual shopping-cart items. The current dataset did not have information on the actual shopping cart items. If such data is made available, a similarity-analysis of shopping cart items can be

performed amongst suspicious transactions. In shopping-cart data analysis, single items may not be as indicative, but information of multiple items can be used to calculate similarity matrices, based on Levenshtein or hamming distances. Further, a comparative analysis of old shopping-cart items with the new ones could be performed. This would definitely throw light on promotional abuse attempts.

This is the first attempt to generate a decision support system for flagging off "first-time promotional discount abuse". The rule-based engine has only been tested on the datasets provided. In large operational data, the rules identified may generate a higher number of false positives and false negatives, respectively. This aspect should be researched in future studies.

6.3 Future scope of the study

Using the rule-based engine, labelling of datasets into genuine and promotional abuse can be performed. Once such labelling is done and the identified labels are verified with actuals, machine learning models may be attempted. Machine learning models will need much large dataset of fraudulent behaviour for its training. Additionally, the study can be extended by performing feature engineering using different pre-processing methods, and new features can be constructed. The new extracted features can be used to make machine learning models for supervised learning exercises. Machine learning address some of the issues which are normally associated with rules-based methods. Focusing on the outcomes rather than the whole decision-making process will make machine learning more robust and less vulnerable to some of the issues that are faced with rules-based systems.

Another thing that can be done once labelled data is made available is working with probabilities. For instance, the chance of fraud from two people sharing the IP address, or the same address can be computed, as such probabilities can be feed into predictive models. This will definitely increase the accuracy of the proposed fraud detection algorithms. A fuzzy logic based approach can also be deployed if probabilities are computed beforehand.

In the current study, the rules identified are for retail e-commerce business. There are several other e-commerce businesses such as food, lodging, health services, web streaming etc. where a lot of first-time discounts are being offered. For instance, in web-streaming business first-time discounts is offered in the form of one-month free-trials. However, abusers use duplicate entries to get continuous free viewership facility after the first-month completion. In such businesses as well, rules-based engines like the current one can be deployed to detect and flag promotional discount abusers.

In summary, the current study addresses for the first time the issue of promotional discount abuses in e-commerce sector. The work discussed a rule-based method for the identification of such abuse cases on real historical transactional data of new customers. Also, the architecture of a proposed information system for detecting such abusers is provided. As fraud detection methods improve, so do the fraudsters, who use altered techniques to defraud websites. The rules identified in this study should, therefore, be updated continuously by generating more rules by experimenting on recent transaction datasets, as it becomes handily available. Even though there exists no detection system which is fool-proof enough to the extent of hundred percent, however, by using a combination of several detection techniques, and further staying guarded for any warning signs, e-commerce companies can possibly decrease the probability of occurrence of such

frauds. The future scope of the study lies in developing a ML model for fraud detection for this problem. Also, a hybrid model incorporating both the rule-based engine and ML models can also be researched upon.

Acknowledgements

The authors would like to acknowledge Mr. Subair Padinchare Porora from Storilabs for his support during the course of the study. The authors also would like to acknowledge Dr. Salwa C.H. for proof reading the manuscript.

References

Aleskerov, E., Freisleben, B. and Rao, B. (1997) 'A neural network based database mining system for credit card fraud detection', *Proceedings of the IEEE/IAFE 1997 Computational Intelligence for Financial Engineering (CIFEr)*, March, IEEE, Cardwatch, pp.220–226.

Amasiatu, C.V. and Shah, M.H. (2014) 'First party fraud: a review of the forms and motives of fraudulent consumer behaviours in e-tailing', *International Journal of Retail & Distribution Management*, Vol. 42, No. 9, pp.805–817.

Assis, C.A., Pereira, A.C., Pereira, M.A. and Carrano, E.G. (2014) 'A genetic programming approach for fraud detection in electronic transactions', *2014 IEEE Symposium on Computational Intelligence in Cyber Security (CICS)*, December, Orlando, FL, IEEE, pp.1–8.

Caldeira, E., Brandao, G. and Pereira, A.C. (2014) 'Fraud analysis and prevention in e-commerce transactions', *2014 9th Latin American Web Congress*, October, Ouro Preto, IEEE, pp.42–49.

Carta, S., Fenu, G., Recupero, D.R. and Saia, R. (2019) 'Fraud detection for E-commerce transactions by employing a prudential multiple consensus model', *Journal of Information Security and Applications*, Vol. 46, pp.13–22.

Chaudhary, K., Yadav, J. and Mallick, B. (2012) 'A review of fraud detection techniques: credit card', *International Journal of Computer Applications*, Vol. 45, No. 1, pp.39–44.

Delamaire, L., Abdou, H. and Pointon, J. (2009) 'Credit card fraud and detection techniques: a review', *Banks and Bank Systems*, Vol. 4, No. 2, pp.57–68.

El Bouchti, A., Chakroun, A., Abbar, H. and Okar, C. (2017) 'Fraud detection in banking using deep reinforcement learning', *2017 Seventh International Conference on Innovative Computing Technology (INTECH)*, August, Luton, IEEE, pp.58–63.

Fakhroutdinov, K. (2020) *UML Use Case Diagram Examples for Online Shopping of Web Customer Actor with Top Level Use Cases View Items, Make Purchase and Client Register, Other Use Cases Are Customer Authentication, View Recommended Items, Add to Wish List, Checkout, Payment Use Case* [online], Uml-diagrams.org, Available at https://www.uml-diagrams.org/examples/online-shopping-use-case-diagram-example.html (Accessed 4 May, 2020).

Fawcett, T. and Provost, F. (1997) 'Adaptive fraud detection', *Data Mining and Knowledge Discovery*, Vol. 1, No. 3, pp.291–316.

Grosan, C. and Abraham, A. (2011) 'Rule-based expert systems', *Intelligent Systems*, Springer, Berlin, Heidelberg, pp.149–185.

Gunasekaran, A. (2020) *The Dark Side of Promo Code Marketing – Razorpay Learn* [online], Razorpay Learn, Available at https://razorpay.com/learn/promo-code-fraud-abuse/ (Accessed 11 May, 2020).

Hao, S., Borgolte, K., Nikiforakis, N., Stringhini, G., Egele, M., Eubanks, M., Krebs, B. and Vigna, G. (2015) 'Drops for stuff: an analysis of reshipping mule scams', *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, Denver, CO, pp.1081–1092.

Huang, S.Y., Lin, C.C., Chiu, A.A. and Yen, D.C. (2017) 'Fraud detection using fraud triangle risk factors', *Information Systems Frontiers*, Vol. 19, No. 6, pp.1343–1356.

Jones, M. (2005) *AI Application Programming*, Charles River Media, Hingham, pp.193–234.

JPMorgan (2020) *E-Commerce Payments Trends: India* [online], Available at: https://www.jpmorgan.com/merchant-services/insights/reports/india (Accessed 4 May, 2020).

Keelery, S. (2020) *India – E-Commerce Market Size 2014–2027|Statista* [online], Available at: https://www.statista.com/statistics/792047/india-e-commerce-market-size (Accessed 4 May, 2020).

Kokkinaki, A.I. (1997) 'On atypical database transactions: identification of probable frauds using machine learning for user profiling', *Proceedings 1997 IEEE Knowledge and Data Engineering Exchange Workshop*, November, IEEE, pp.107–113.

Kou, Y., Lu, C.T., Sirwongwattana, S. and Huang, Y.P. (2004) 'Survey of fraud detection techniques', *IEEE International Conference on Networking, Sensing and Control*, *2004*, March, IEEE, Vol. 2, pp.749–754.

Kundu, A., Panigrahi, S., Sural, S. and Majumdar, A.K. (2009) 'Blast-ssaha hybridization for credit card fraud detection', *IEEE Transactions on Dependable and Secure Computing*, Vol. 6, No. 4, pp.309–315.

Lebichot, B., Le Borgne, Y.A., He-Guelton, L., Oblé, F. and Bontempi, G. (2019) 'Deep-learning domain adaptation techniques for credit cards fraud detection', *INNS Big Data and Deep Learning Conference*, April, Springer, Cham, pp.78–88.

Lek, M., Anandarajah, B., Cerpa, N., and Jamieson, R. (2001) 'Data mining prototype for detecting ecommerce fraud', ın Smithson, S., Gricar, J., Podlogar, M. and Avgerinou, S. (Eds.): *Proceedings of the 9th European Conference on Information Systems, Global Co-operation in the New Millennium, ECIS 2001*, Bled, Slovenia, 27–29 June, pp.160–165.

Leonard, K.J. (1995) 'The development of a rule-based expert system model for fraud alert in consumer credit', *European Journal of Operational Research*, Vol. 80, No. 2, pp.350–356.

Lima, R.F. and Pereira, A.C. (2016) 'Feature selection approaches to fraud detection in e-payment systems', *International Conference on Electronic Commerce and Web Technologies*, September, Springer, Cham, pp.111–126.

Mead, A., Lewris, T., Prasanth, S., Adams, S., Alonzi, P. and Beling, P. (2018) 'Detecting fraud in adversarial environments: A reinforcement learning approach', *2018 Systems and Information Engineering Design Symposium (SIEDS)*, April, Charlottesville, VA, IEEE, pp.118–122.

Phua, C., Smith-Miles, K., Lee, V. and Gayler, R. (2010) 'Resilient identity crime detection', *IEEE Transactions on Knowledge and Data Engineering*, Vol. 24, No. 3, pp.533–546.

Polman, T. and Spruit, M. (2013) 'Integrating knowledge engineering and data mining in e-commerce fraud prediction', *World Summit on Knowledge Society*, September, Springer, Berlin, Heidelberg, pp.460–466.

Porwal, U. and Mukund, S. (2019) 'Credit Card Fraud Detection in E-Commerce', *2019 18th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/13th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE)*, August, Rotorua, New Zealand, IEEE, pp.280–287.

Quah, J.T. and Sriganesh, M. (2008) 'Real-time credit card fraud detection using computational intelligence', *Expert Systems with Applications*, Vol. 35, No. 4, pp.1721–1732.

Rajeshwari, U. and Babu, B.S. (2016) 'Real-time credit card fraud detection using streaming analytics', *2016 2nd International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT)*, July, Bangalore, IEEE, pp.439–444.

Rezaee, Z. (2002) *Financial Statement Fraud: Prevention and Detection*, John Wiley & Sons, New York, NY.

Rosset, S., Murad, U., Neumann, E., Idan, Y. and Pinkas, G. (1999) 'Discovery of fraud rules for telecommunications – challenges and solutions', *Proceedings of the Fifth ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, August, San Diego, CA, pp.409–413.

Saia, R. and Carta, S. (2019) 'Evaluating the benefits of using proactive transformed-domain-based techniques in fraud detection tasks', *Future Generation Computer Systems*, Vol. 93, pp.18–32.

Shaji, J. and Panchal, D. (2017) 'Improved fraud detection in e-commerce transactions', *2017 2nd International Conference on Communication Systems, Computing and IT Applications (CSCITA)*, April, Mumbai, IEEE, pp.121–126.

Shopify Developers (2020) *Order* [online], Available at: https://shopify.dev/docs/admin-api/rest/reference/orders/order (Accessed 4 May, 2020).

Srivastava, A., Kundu, A., Sural, S. and Majumdar, A. (2008) 'Credit card fraud detection using hidden Markov model', *IEEE Transactions on Dependable and Secure Computing*, Vol. 5, No. 1, pp.37–48.

Tao, J., Wang, H. and Xiong, T. (2018) 'Selective graph attention networks for account takeover detection', *2018 IEEE International Conference on Data Mining Workshops (ICDMW)*, November, IEEE, Singapore, pp.49–54.

Wang, J.H., Liao, Y.L., Tsai, T.M. and Hung, G. (2006) 'Technology-based financial frauds in Taiwan: issues and approaches', *2006 IEEE International Conference on Systems, Man and Cybernetics*, IEEE, October, Vol. 2, pp.1120–1124.

Wang, X., Zhang, L. and Liu, Y. (2017) 'Research and design of a rules engine for bank anti-fraud platform', *2016 International Conference on Engineering Management (Iconf-EM 2016)*, January, Guangzhou, Atlantis Press, pp,247–252.

Wheeler, R. and Aitken, S. (2000) 'Multiple algorithms for fraud detection', *Applications and Innovations in Intelligent Systems VII*, Springer, London, pp.219–231.

Xuan, S., Liu, G., Li, Z., Zheng, L., Wang, S. and Jiang, C. (2018) 'Random forest for credit card fraud detection', *2018 IEEE 15th International Conference on Networking, Sensing and Control (ICNSC)*, March, Zhuhai, IEEE, pp.1–6.

Ye, N., Vilbert, S. and Chen, Q. (2003) 'Computer intrusion detection through EWMA for autocorrelated and uncorrelated data', *IEEE Transactions on Reliability*, Vol. 52, No. 1, pp.75–82.

Zhao, J., Lau, R.Y., Zhang, W., Zhang, K., Chen, X. and Tang, D. (2016) 'Extracting and reasoning about implicit behavioral evidences for detecting fraudulent online transactions in e-commerce', *Decision Support Systems*, Vol. 86, pp.109–121.