Dragan Stojković, Zoran Bogetić, Aleksa Dokić: ANALYZING FIRST PARTY FRAUD AS ONE OF THE KEY CHALLENGES OF FORENSIC PROCESS IN E-TAILING

ANALIZA DIREKTNE PREVARE LICA KAO KLJUČNOG IZAZOVA FORENZIČKOG PROCESA U ELEKTRONSKOJ MALOPRODAJI

Dragan Stojković[49], Zoran Bogetić,[50] Aleksa Dokić[51]

Abstract: E-tailers, both brick-and-click and pure-click, are faced with the rising threat of first-party fraud. This has been due to many factors, such as the anonymity of the internet and a large volume of daily transactions. Since the damages and implications of first-party fraud are significant in e-tailing industry, the incentive is high to improve and optimize existing fraud management frameworks for tackling the aforementioned fraudulent activities. To this end, the existing literature has been thoroughly analyzed in order to identify relevant steps and activities of first-party fraud management in e-tail. The final outcome of the paper is the proposition of the stepwise implementation procedure for first-party fraud handling in e-tail. Both practitioners and scientist can benefit from the findings, as they represent a solid basis of further analysis of this topic, as well as the foundation for expanding the fraud management framework to other relevant aspects.
Keywords: e-tailing, first-party fraud, forensic process, fraud management, pure-click retail, brick-and-click retail
JEL classification: M10, M15, M4

Apstrakt: E-trgovci, kako brick-and-click tako i pure-click, suočavaju se sa rastućom pretnjom od direktnih prevara lica. Uzroci ovoga su mnogi, poput anonimnosti interneta i velikog broja dnevnih transakcija. S obzirom da su štete i implikacije ovog vida prevare u e-maloprodaji značajni, postoji velika motivacija za unapređenjem i optimizacijom postojećih okvira za rešavanje i upravljanje prevarama. Stoga je postojeća literatura detaljno analizirana kako bi se identifikovali relevantni koraci i aktivnosti rešavanja i upravljanja direktnim prevarama lica u elektronskoj maloprodaji. Konačni ishod ovog rada jeste predlog fazne primene procedure za rešavanje ovih prevara u e-maloprodaji. Profesionalci i istraživači mogu imati koristi od dobijenih nalaza, pošto predstavljaju solidnu osnovu za dalju analizu ove oblasti, kao i polaznu tačku za dalje proširenje okvira za upravljanje prevarama u drugim relevantnim aspektima.
Ključne reči: e-maloprodaja, direktna prevara lica, forenzički proces, menadžment rešavanje prevara, internet maloprodaja, višekanalna maloprodaja
JEL klasifikacija: M10, M15, M4

[49] University of Belgrade - Faculty of Economics and Business, dragan.stojkovic@ekof.bg.ac.rs
[50] University of Belgrade - Faculty of Economics and Business, zoran.bogetic@ekof.bg.ac.rs
[51] University of Belgrade - Faculty of Economics and Business, aleksa.dokic@ekof.bg.ac.rs

1. Introduction

As many retailers intensify their online channel sales efforts, they are consequently faced with the increasing number of ever more complex frauds. Due to the nature of retail business, one of the most important types of fraudulent activities in e-tailing is first-party fraud. Forensic accounting represents a combination of financial and investigative techniques aimed at discovering, evaluating and tackling various forms of financial criminal activities, such as first-party fraud. As frauds take up a significant portion of all financial crimes, the goal of forensic process in fraud management is to provide the necessary expertise to detect, investigate, mitigate and sometimes even prevent fraudulent activities. To this end, forensic process in e-tailing relies on a skillset which enables effective anti-fraud activities. With the rapid development of online business, many industries have turned towards various forms of pure-click or multiple-channel business models. It is not surprising that we are seeing a growing number of papers observing the important role of forensic accounting in this context. Due to the nature and intensity of financial transactions, the majority of papers investigates the role of forensic accounting in financial institutions (Abdulrahman, 2019; Aigienohuwa et al., 2017; Bassey, 2018; Eko et al., 2020; Henry & Ganiyu, 2017). However, papers observing the role of forensic accounting in retail fraud management are somewhat lacking.

For this reason, it is important to explore the current state of knowledge regarding forensic accounting, as well as existing first-party fraud management frameworks in e-tailing, in order to provide a critical overview of the potential forensic accounting applications and future research directions. This paper builds upon this research gap and contributes to the existing literature by summarizing and explaining the existing forms of first-party fraud in retail, as well as by proposing the stepwise implementation framework for tackling these fraudulent activities.

2. First party fraud in e-tailing

First-party fraud encompasses fraudulent activities perpetrated by individuals using their own identity and personal information, rather than fake identity, stolen identity or third-parties (Amasiatu & Shah, 2018). First-party fraud is oftentimes more difficult to detect and prevent than third-party fraud as it entails the use of personal, legitimate information by the fraudster. First-party fraud has been examined from many different perspectives, such as behaviorism, criminology and computer sciences. However, understanding the implications of first-party fraud from the retail perspective is constantly gaining in importance, especially in the context of e-tailing development. Retail context implies that the fraudster uses personal information to obtain products or services with no intention of fulfilling the payment or abiding by the merchant's terms and conditions.

First-part fraud in retail has come a long way from simple physical forms, such as shoplifting. With the rapid expansion of e-tailing, both brick-and-click and pure-click retailers are exposed to a wide variety of online fraudulent activities committed by their customers. It is becoming increasingly difficult to detect and prevent first-party fraud in e-commerce, mainly due to the high volume of transactions and the anonymity of the internet (Soomro et al., 2019). This is why first-party fraud has become a significant limiting factor in e-tail development, especially in developing and emerging markets characterized by lagging and inadequate legislation.

Some earlier papers focused on fraudulent behaviors in retail point out activities such as shoplifting (Bamfield, 2004) and deshopping (King et al., 2007; Reynolds & Harris, 2005). These activities represent types of aberrant consumer behaviors, predominantly property abuse and dishonest acts (Harris & Daunt, 2011). However, these papers observe fraudulent activities from the general retail point of view. E-tail, especially omni-channel retail, has many specific characteristics that create a very challenging environment in terms of fraud susceptibility, much more so than brick-and-mortar retail. Therefore, it is important to fully understand occurring fraudulent situations in e-tailing.

A *chargeback fraud* is one of the most common first-party fraud types in which a customer disputes a charge with their credit card company / bank related to a regularly made product or service purchase (John et al., 2020). In the majority of cases the customer makes a claim that the performed transaction was not authorized, or that the ordered product was not received (Liu & Lee, 2022). In certain instances, chargeback fraud is referred to as a friendly fraud, whereas in other situations it is seen as a subtype of friendly fraud, differentiated from it by the existence of malicious intent. Whatever the case, the negative implications of this activity based on customer protection legislation are apparent (Vivian Amasiatu & Hussain Shah, 2014). Some data shows that the friendly fraud has become the largest source of frauds in retail (39% of retail experiencing in 2021), as 2.6% of all e-commerce transactions have led to chargebacks in Europe (CyberSource Corporation, 2021). Chargeback fraud will definitely remain one of the main challenges for e-tailers, as it currently accounts between 40% to 80% of all losses attributed to e-commerce fraud (Columbus, 2020).

Very similar in nature is the *refund fraud*. Unlike the previous type of fraud, refund scamming occurs when a customer requests a refund for the received product or service, on the false account of it being defective, damaged or not received (John et al., 2020). Upon receiving the refund, the customer fails to return the product, oftentimes providing false information, such as fake tracking number. Around 27% of retailers globally have been exposed to this type of fraudulent behavior (CyberSource Corporation, 2021)

Deshopping represents a situation in which a customer deliberately returns a product after use in order to receive full reimbursement (Schmidt et al., 1999). E-tailing is especially susceptible to this kind of behavior, due to strict refund legal treatments (King et al., 2007). The occurrence of deshopping is heavily motivated by the existence of liberal return policies of e-tailers (Amasiatu & Shah, 2019). Some older studies showed that every fifth return in retail is fraudulent in nature (Piron & Young, 2000). Newer data suggests that fraudulent returns are predominantly perpetrated by frequent returners who, although spend more, return most or all of the ordered products (Foscht et al., 2013).

Misuse of facility accounts for almost one fifth of all frauds, with 79,000 registered cases in 2021 in UK (CIFAS, 2022). As 88% of these cases are associated with bank accounts, it is no wonder that bust-out customers perpetrating this fraud pose a serious threat to e-commerce development. Basically, this fraudulent activity occurs when a customer acquires a credit facility, either from a bank, retailer, or some other crediting institution, without the intention of fulfilling obligations stipulated by the crediting agreement (Vivian Amasiatu & Hussain Shah, 2014). The reason why these bust out schemes can be so damaging lies in the difficulty of its detection, and consequent obtaining of the proof of intent (Hoffmann & Birnbrich, 2012). Closely related fraudulent behavior is the *misrepresentation of details*, in which a customer provides false, or hides real personal data in order to access facilities otherwise unobtainable (Whitehead, 2021).

Finally, one especially damaging fraud type to e-tailers, as it potentially endangers their brand perception, alongside incurred financial losses, is *triangulation scheme*. This fraudulent activity is on the rise as every fifth retailer globally is exposed to it (CyberSource Corporation, 2021). Triangulation fraud is a complex intermediation scheme in which a fraudster establishes a fake e-store, or some other online sales platform. Upon receiving the order via this fake platform, the fraudster then orders the same product from a legitimate retailer and has it shipped to its customer's address, whilst keeping the received payment for the sent product for himself (Chua & Wareham, 2004).

Finally, a fraudster can use stolen credit card information in order to make a small, "under the radar" purchase (Saluja, 2022). The idea behind this *card testing* activity is to check whether the stolen credit

card is still valid, so that it can be used for high-amount purchases (Patidar & Sharma, 2011). Card testing represents a second most common fraud, as 37% of retailers have come into contact with this fraudulent activity (CyberSource Corporation, 2021).

As we can see, first-party fraud comes in many different forms, affecting many business sectors, such as retail, wholesale, financial, banking, real-estate and servicing. Within these, e-tailers are especially vulnerable to first-party frauds, due to the very nature of e-commerce transactions. Firstly, e-commerce transactions are remote in nature, as they require no face-to-face interactions between buyer and sellers. Secondly, e-commerce transactions rely heavily on electronic payment, especially the use of credit cards. This, coupled with the fact that customers are often required to provide personal information, creates significant room for the occurrence of first-party fraud, especially the ones related to credit card use. Also, e-tailers have been faced with the increasing number of daily transactions, especially during and after the pandemic. High order volume limits the potential for manual transaction data check-up, allowing many first-party fraudster to remain undetected. Finally, strict national legislation, such as the one related to online retailer's return policy, can have a negative effect by motivating fraudsters to take advantage of it. This is very damaging for e-tailers, as activities such as refund fraud, deshopping and chargeback fraud are on the rise.

By analyzing the specific characteristics of e-commerce transactions, we can understand how and why e-tailers are susceptible to first-party fraud. This is a vital precondition in order to be able to identify adequate prevention and detection strategies aimed at handling first-party fraud in e-tail.

3. First-party fraud management aspect of forensic process in e-tailing

We have seen that first-party fraud in e-commerce entails many different types of activities and behavior. As such, these fraudulent activities have driven e-tailers to develop various responses. Retailers' responses in this regard are aimed at both preventing and managing first-party fraud.

The first step, and oftentimes the most difficult is to detect a fraudulent activity. The idea behind first-party fraud detection is to analyze the customer and transaction data in order to identify suspicious, potentially fraudulent behavioral patterns (Rezaee & Wang, 2019). Nowadays, e-tailers' analytical power and data processing capacity are greatly expanded through the use of advanced analytics and machine learning algorithms, which allows for more in-depth approach to pointing out anomalies and "red flags" in customer online purchasing behavior. However, not all suspicious behavior is fraudulent. Therefore, a deeper analysis is required in order to differentiate between fraud and inconsistency.

Each suspicious situation should be investigated for the presence of fraudulent elements. This is the most complex aspect of fraud management for the retailer, as the success relies heavily on data gathering. If the information acquired by observing transaction history and customer identity data, as well as through communication with the customer, do not portray a clear picture of what has occurred within the transaction in question, the application of forensic techniques is difficult (Rezaee & Wang, 2019). Additionally, the lack of data can lead to a situation in which a retailer has a reasonable doubt that first-party fraud has occurred, but cannot prove it. Due to these situations, it is prudent to invest more in establishing stricter anti-fraud procedures, such as advanced authentication and verification processes, introducing advanced fraud detection techniques and training employees in forensic accounting techniques for managing fraudulent behavior (Ehioghiren & Atu, 2016).

If the first-party fraud has indeed occurred and been confirmed, retailers are faced with the problem of how to best mitigate the negative effects caused by the fraud. The aim of this step is to minimize the risk exposure and financial losses facing the e-tailer. In this sense, by evaluating the total damages, retailer can opt to implement various responses to fraud, ranging from transaction cancellation and

customer account blacklisting, to initiating a refund procedure or taking legal actions against the fraudster.

Presented retailer's responses are oftentimes combined and simultaneously or consequently applied through various fraud management frameworks. One of the most famous, as well as comprehensive outlines for handling fraudulent activity is provided by Wilhelm (2004), as it entails everything from deterrence to prosecution (**Figure 1**).

Figure 1. Representation of the fraud management lifecycle

Source: Wilhelm (2004)

Fraud management lifecycle theory proposed by Wilhelm (2004) has many merits, especially in terms of defining key steps in resolving fraudulent activity, as well as standardizing the fraud management process. However, the presented framework is developed for fraudulent activities in general, not first-party fraud specifically. Secondly, observed responses go beyond the scope of e-tailer's activities. These moments are not shortcomings per se, but do somewhat limit the application of the framework in the context of first-party fraud.

A more specialized model has been proposed by Amasiatu & Shah (2018). This framework is adapted to suit specificities of the retail industry, and is thus much more applicable in e-tail context compared to the previous one. Additionally, the framework builds upon the one by Wilhelm (2004), focusing on retailer's activities and responses, further expanding the process of investigating, sanctioning and evaluating first-party fraud and its effects (**Figure 2**).

Figure 2. Representation of the first-party fraud management in retail industry

Source: Amasiatu & Shah (2018)

As the aim of this paper is to identify the forensic process for coping with first-party fraud in e-tail, we focus on the activities within the first-party fraud management framework where forensic accounting can be used. These include first party fraud detection, investigation and mitigation.

a. First-party fraud detection in e-tail

As explained, detection is one of the key aspects of first-party fraud management. E-tailers must constantly be on the lookout for suspicious activities and characteristics telltale signs of fraudulent behavior. Detection, however, is not always easy, especially due to the rising complexity of online transactions. Therefore, e-tailers oftentimes include various steps preceding online transactions, such as identity verification, different types of authentications, analysis of behavioral data, as well as transaction risk scoring. By introducing these transaction checkpoints, e-tailers reduce the possibility of fraudulent activity occurring "under the radar".

The underlined idea for the e-tailer is to gather various data related to the specific customer and transaction in order to create a database capable of providing early warning system capability. To detect first-party fraud through data collection and management, e-tailers implement various techniques. Some of the most common ones are (modified from Singh & Singh, 2015):

- Address Verification System (AVS)

- Velocity checking
- IP address monitoring
- Transaction value check
- Mobile device fingerprinting
- Public database cross-referencing
- Customer behavior mapping

All these techniques provide valuable information on e-tailer's customers. By knowing the expected customer behavior, e-tailer will be able to detect potential fraud if specific customer activity differs from expected patterns. These "red flags" are the primary points for further investigation.

The key challenges for e-tailers regarding fraud detection are to create sufficiently precise evaluations of customer behavioral patterns, as well as to implement a fast and responsive information system capable of providing instant notifications in case of potential fraud occurrence. To this end, fraud detection has been a fruitful scientific field for implementing various methodologies aimed at overcoming these challenges. Sahin & Duman (2011) implemented artificial neural networks with logistic regression in order to tackle the problem of credit card fraud detection. Similarly, Patidar & Sharma (2011) also proposed a credit card fraud detection framework based on neural networks. Machine learning algorithms have also been developed for this purpose (Banerjee et al., 2018), as well as fuzzy frameworks (Askari & Hussain, 2017) and certain graphical solutions (Sadowksi & Rathle, 2015).

The role of forensic accounting within the first-party fraud detection phase is very important. Based on the estimations, as well as previous cases, forensic accountant can provide a comprehensive list of parameters and indicators which are indicative of fraudulent activity, as well as how to evaluate and use them (Kaur et al., 2023). These indicators should be closely monitored by the e-tailer, and when a specific indicator goes beyond the evaluated critical threshold, further investigation into a specific transaction should be triggered.

b. First-party fraud investigation in e-tail

Investigative phase basically entails three main steps – further data gathering, data analysis and decision making. Upon coming onto a suspicious transaction e-tailer's first task should be to gather as much of relevant data on the transaction and customer in question as possible. Alongside basic information, such as customer account history, this search should follow a precise line guided by the list of fraud indicators. To this end, an e-tailer should identify whether the suspicious transaction is characterized by (modified from Singh & Singh, 2015):

- Inconsistent customer personal information
- Use of temporary email address
- Use of proxy servers or VPNs
- Inconsistencies in terms of purchasing patterns
- Failed verification steps

These, coupled with many other relevant indicators provide a clear image of the suspicious transaction and provide a solid base for verification process.

Upon analyzing the available data and comparing it to relevant value thresholds, the e-tailer is faced with a decision – are there enough elements to suspect a first-party fraud. If the answer is positive, a decision should be made on how to proceed. Depending on various factors, the e-tailer can cancel the transaction, ask for chargeback or pursue further legal activities (Amasiatu & Shah, 2019). Forensic accounting is of vital importance in this stage of first-party fraud management. Firstly, forensic accounting provides an insight into relevant signals and indicators of fraudulent behavior within the

transaction. Secondly, forensic accounting consists of important guidelines for data gathering, data analysis and evaluation, as well as decision making. Closely related to the investigative role of forensic accounting is also its capacity to evaluate the effects of each fraudulent transaction in monetary terms (Kaur et al., 2023).

c. First-party fraud mitigation in e-tail

First-party mitigation accounts for activities ranging from fraud damage evaluation to choosing the sanctioning and redress. In this sense, forensic accountants can use their expertise to assess the risk of a specific transaction, negative monetary effects and damages of the committed fraud, as well as the cost-benefit analysis of available responses to the fraud (Utomwen & Danjuma, 2015).

Risk evaluation in e-tail is a very complex matter, depending on a large number of factors. The longer the fraud detection time and fraudulent transaction progress, the higher the exposure, and thus risk for the e-tailer (Chepkoech & Rotich, 2017). Also, the type of first-party fraud plays a significant role in determining the transaction risk level. Forensic accountant must take into account all relevant transaction-related data and provide real-time risk profiling and exposure assessment (Yang & Lee, 2020).

Upon determining the transaction risk, as well as incurred damages caused by the first-party fraud, the e-tailer must choose how to respond to the fraud. In case of early detection, simple customer account blockage or transaction cancelation is a viable option, However, if the transaction has already taken place, e-tailers are faced with a dilemma of whether to search for ways of reimbursement, if possible, seek legal protection, or simply cut the losses and move on (Utomwen & Danjuma, 2015). Forensic accounting can help significantly in this regard, as cost-benefit analysis of responses to fraudulent activities is an integral part of the field. Additionally, should any legal activities be undertaken, forensic accounting can provide expert testimony of the investigation process, as well as incurred costs.

4. Conclusion and future research

The pace of B2C e-commerce development intensified the need for a comprehensive, thorough approach towards the increasing number of first-party frauds. The conducted analysis showed that first-party fraud comes in many different shapes and sizes, contributing to the overall complexity of fraud management in e-tail. Modern technologies and large volume of online retail transactions create many gaps in e-tailers' defenses for fraudsters to exploit.

Strategic and proactive implementation of forensic accounting principles and practices within the first-party fraud management has become a must-have, especially for e-tailers dealing with a large number of orders on a daily basis. As we have seen, forensic accounting has the most prominent implementation within the activities of first-party fraud detection, investigation and mitigation.

Forensic process has both an operative and a strategic component within the first-party fraud management. The operative component reflects the activities aimed at observing and analyzing transaction-specific data. The aim of this aspect is to provide a responsive early warning system in case of fraud occurrence, as well as to process each suspicious transaction. The specificities of e-tailing are important to consider in this aspect. Online transactions are quick passed and require no physical contact, making fraud detection harder. Additionally, digital environment is more prone to complex forms of fraud compared to physical retail. Finally, online transactions are characterized by digital data only, thus eliminating the intuition of the employees to detect potential fraud face-to-face.

If the online fraud transpired, forensic activities take on a new roll, predominantly aimed at containing financial damage incurred, as well as provide a detailed account of the fraudulent activities which took

place. This is an important step, as it also has strategic implications. After identifying modus operandi of the fraudster, e-tailer should always update its corporate security policy, based on the forensic recommendations (Kabuye et al., 2017). These recommendations include what to look after, how to respond to specific red flags, etc. and should be introduced and updated on the regular basis within the detection phase of the first-party fraud management. The overall recommended forensic process for e-tailers tackling first-party fraud is depicted in **Figure 3**.

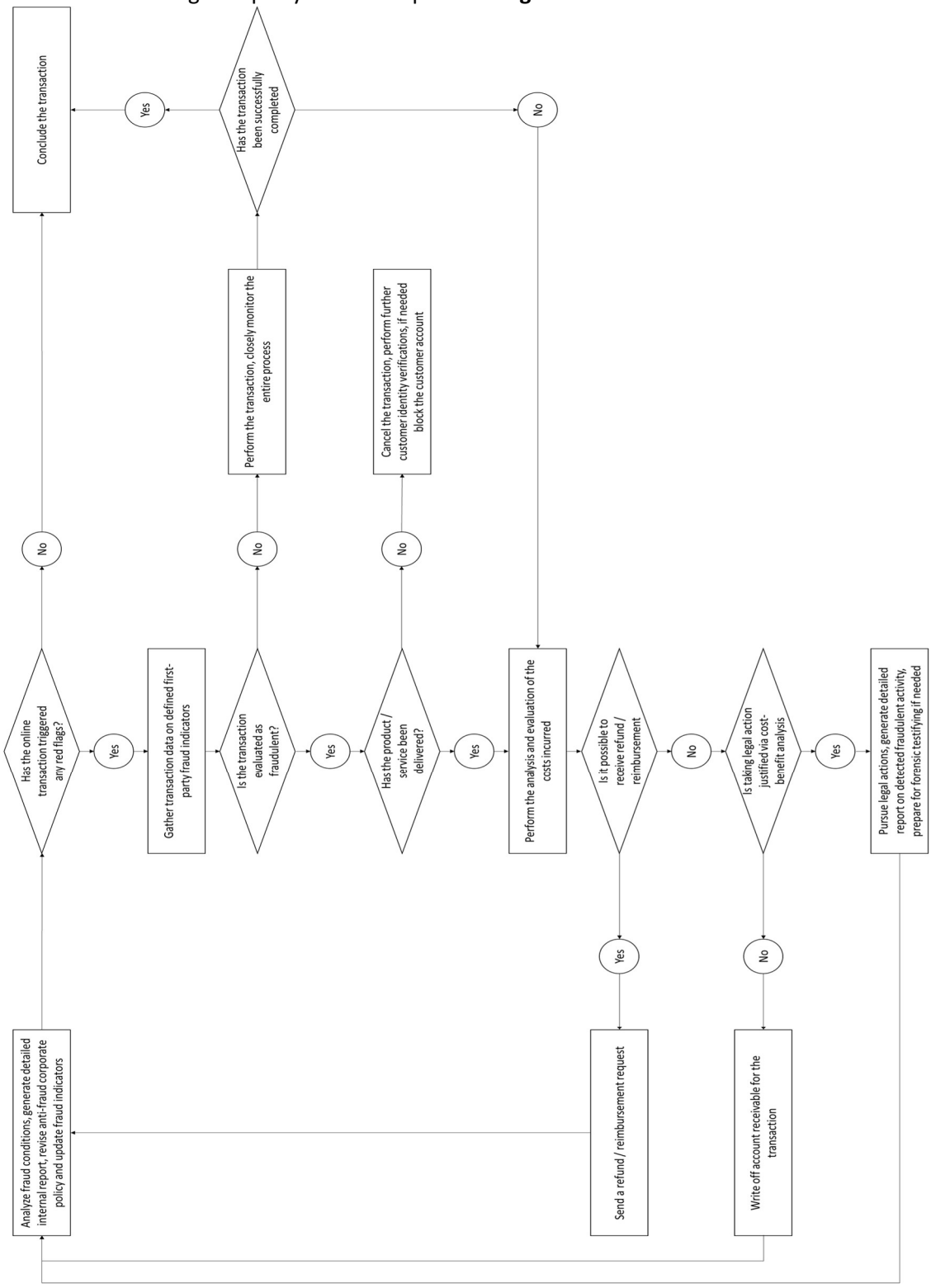

Figure 3. Forensic process stepwise implementation within the first-party fraud management framework in e-tailing

Forensic process entails a set of financial and investigative techniques. As the fraud data in e-tail are digital in nature, and oftentimes real-time and instant (Rezaee & Wang, 2019), there is a significant incentive to explore the implementation potential of various MCDA, AI and analytical methodologies. These methodologies are aimed at processing a large quantity of data in a multiple criteria manner, with the aim of optimizing decision-making process. Many authors have already explored the use of techniques, such as machine learning and neural networks. These models represent a good foundation for further research into this field, especially when considering the specificities of first-party fraud in e-tail. This would be a very beneficial research avenue in the managerial sense, as the fraudsters would be disincentivized. Reduction in the annual number of frauds would enable further expansion of online retail and improve the overall security level of the national and international e-market.

Literature

1. Abdulrahman, S. (2019). Forensic accounting and fraud prevention in Nigerian public sector: A conceptual paper. *International Journal of Accounting & Finance Review*, *4*(2), 13–21.
2. Aigienohuwa, O., Okoye, E. I., & Uniamikogbo, E. O. (2017). Forensic accounting and fraud mitigation in the Nigerian banking industry. *Accounting and Taxation Review*, *1*(1), 177–195.
3. Amasiatu, C. V., & Shah, M. H. (2018). First party fraud management: Framework for the retail industry. *International Journal of Retail & Distribution Management*, *46*(4), 350–363. https://doi.org/10.1108/IJRDM-10-2016-0185
4. Amasiatu, C. V., & Shah, M. H. (2019). The management of first party fraud in e-tailing: A qualitative study. *International Journal of Retail & Distribution Management*, *47*(4), 433–452. https://doi.org/10.1108/IJRDM-07-2017-0142
5. Askari, S. Md. S., & Hussain, Md. A. (2017). Credit card fraud detection using fuzzy ID3. *2017 International Conference on Computing, Communication and Automation (ICCCA)*, 446–452. https://doi.org/10.1109/CCAA.2017.8229897
6. Bamfield, J. (2004). Shrinkage, shoplifting and the cost of retail crime in Europe: A cross-sectional analysis of major retailers in 16 European countries. *International Journal of Retail & Distribution Management*, *32*(5), 235–241. https://doi.org/10.1108/09590550410699233
7. Banerjee, R., Bourla, G., Chen, S., Kashyap, M., & Purohit, S. (2018). Comparative Analysis of Machine Learning Algorithms through Credit Card Fraud Detection. *2018 IEEE MIT Undergraduate Research Technology Conference (URTC)*, 1–4. https://doi.org/10.1109/URTC45901.2018.9244782
8. Bassey, E. B. (2018). Effect of forensic accounting on the management of fraud in microfinance institutions in Cross River State. *Journal of Economics and Finance*, *9*(4), 79–89.
9. Chepkoech, F., & Rotich, G. (2017). Effect of risk management process on motor insurance fraud in Kenya. *International Journal of Social Sciences and Information Technology*, *3*(3), 1934–1951.
10. Chua, C. E. H., & Wareham, J. (2004). Fighting Internet auction fraud: An assessment and proposal. *Computer*, *37*(10), 31–37. https://doi.org/10.1109/MC.2004.165
11. CIFAS. (2022). *Fraudscape 2022*. https://www.fraudscape.co.uk/#welcome
12. Columbus, L. (2020). *How E-Commerce's Explosive Growth Is Attracting Fraud*. Forbes. https://www.forbes.com/sites/louiscolumbus/2020/05/18/how-e-commerces-explosive-growth-is-attracting-fraud/
13. CyberSource Corporation. (2021). *2021 Global Fraud Report*. https://www.cybersource.com/content/dam/documents/campaign/global-fraud-report-2021.pdf
14. Ehioghiren, E. E., & Atu, O. O. K. (2016). Forensic accounting and fraud management: Evidence from Nigeria. *Igbinedion University Journal of Accounting*, *2*(8), 245–308.
15. Eko, E. U., Adebisi, A. W., & Moses, E. J. (2020). Evaluation of forensic accounting techniques in fraud prevention/detection in the banking sector in Nigeria. *International Journal of Finance and Accounting*, *9*(3), 56–66.
16. Foscht, T., Ernstreiter, K., Maloles, C., Sinha, I., & Swoboda, B. (2013). Retaining or returning? Some insights for a better understanding of return behaviour. *International Journal of Retail & Distribution Management*.
17. Harris, L. C., & Daunt, K. L. (2011). Deviant customer behaviour: A study of techniques of neutralisation. *Journal of Marketing Management*, *27*(7–8), 834–853. https://doi.org/10.1080/0267257X.2010.498149
18. Henry, A. W., & Ganiyu, A. B. (2017). Effect of forensic accounting services on fraud reduction in the Nigerian banking industry. *Advances in Social Sciences Research Journal*, *4*(12).
19. Hoffmann, A. O. I., & Birnbrich, C. (2012). The impact of fraud prevention on bank-customer relationships: An empirical investigation in retail banking. *International Journal of Bank Marketing*, *30*(5), 390–407. https://doi.org/10.1108/02652321211247435
20. John, S., Shah, B. J., & Kartha, P. (2020). Refund fraud analytics for an online retail purchases. *Journal of Business Analytics*, *3*(1), 56–66. https://doi.org/10.1080/2573234X.2020.1776164

21. Kabuye, F., Nkundabanyanga, S. K., Opiso, J., & Nakabuye, Z. (2017). Internal audit organisational status, competencies, activities and fraud management in the financial services sector. *Managerial Auditing Journal*, *32*(9), 924–944. https://doi.org/10.1108/MAJ-09-2016-1452
22. Kaur, B., Sood, K., & Grima, S. (2023). A systematic review on forensic accounting and its contribution towards fraud detection and prevention. *Journal of Financial Regulation and Compliance*, *31*(1), 60–95.
23. King, T., Dennis, C., & McHendry, J. (2007). The management of deshopping and its effects on service: A mass market case study. *International Journal of Retail & Distribution Management*.
24. Liu, D., & Lee, J.-H. (2022). CFLedger: Preventing chargeback fraud with blockchain. *ICT Express*, *8*(3), 352–356. https://doi.org/10.1016/j.icte.2021.06.001
25. Patidar, R., & Sharma, L. (2011). Credit Card Fraud Detection Using Neural Network. 1.
26. Piron, F., & Young, M. (2000). Retail borrowing: Insights and implications on returning used merchandise. *International Journal of Retail & Distribution Management*.
27. Reynolds, K. L., & Harris, L. C. (2005). When service failure is not service failure: An exploration of the forms and motives of "illegitimate" customer complaining. *Journal of Services Marketing*.
28. Rezaee, Z., & Wang, J. (2019). Relevance of big data to forensic accounting practice and education. *Managerial Auditing Journal*, *34*(3), 268–288.
29. Sadowksi, G., & Rathle, P. (2015). Fraud Detection: Discovering Connections with Graph Databases. *Neo4j*.
30. Sahin, Y., & Duman, E. (2011). Detecting credit card fraud by ANN and logistic regression. *2011 International Symposium on Innovations in Intelligent Systems and Applications*, 315–319. https://doi.org/10.1109/INISTA.2011.5946108
31. Saluja, S. (2022). Identity theft fraud- major loophole for FinTech industry in India. *Journal of Financial Crime*. https://doi.org/10.1108/JFC-08-2022-0211
32. Schmidt, R. A., Sturrock, F., Ward, P., & Lea-Greenwood, G. (1999). Deshopping–the art of illicit consumption. *International Journal of Retail & Distribution Management*, *27*(8), 290–301.
33. Singh, P., & Singh, M. (2015). Fraud Detection by Monitoring Customer Behavior and Activities. *International Journal of Computer Applications*, *111*(11), 23–32. https://doi.org/10.5120/19584-1340
34. Soomro, Z. A., Ahmed, J., Shah, M. H., & Khoumbati, K. (2019). Investigating identity fraud management practices in e-tail sector: A systematic review. *Journal of Enterprise Information Management*, *32*(2), 301–324. https://doi.org/10.1108/JEIM-06-2018-0110
35. Utomwen, O., & Danjuma, E. (2015). The role of forensic accounting in mitigating financial crimes. *International Journal of Commerce and Management Research*, *1*(1), 40–47.
36. Vivian Amasiatu, C., & Hussain Shah, M. (2014). First party fraud: A review of the forms and motives of fraudulent consumer behaviours in e-tailing. *International Journal of Retail & Distribution Management*, *42*(9), 805–817. https://doi.org/10.1108/IJRDM-05-2013-0112
37. Whitehead, E. (2021). Why e-commerce attracts fraud. *Computer Fraud & Security*, *2021*(10), 6–7. https://doi.org/10.1016/S1361-3723(21)00106-8
38. Wilhelm, W. K. (2004). The fraud management lifecycle theory: A holistic approach to fraud management. *Journal of Economic Crime Management*, *2*(2), 1–38.
39. Yang, C.-H., & Lee, K.-C. (2020). Developing a strategy map for forensic accounting with fraud risk management: An integrated balanced scorecard-based decision model. *Evaluation and Program Planning*, *80*, 101780.