East African Journal of Information Technology
eajit.eanso.org
Volume 7, Issue 1, 2024
Print ISSN: 2707-5346 | Online ISSN: 2707-5354
Title DOI: https://doi.org/10.37284/2707-5354

EAST AFRICAN NATURE & SCIENCE ORGANIZATION

Original Article

Assessing Mobile Network Fraud Threats and Prevention Strategies in Kenya

James Mundia[1], Evans Kirimi Miriti[1], Stephen Mburu[1], Andrew Mwaura Kahonge[1] & Christopher Kipchumba Chepken[1]*

[1] University of Nairobi, P. O. Box 30197-00100. Nairobi, Kenya.
* Corresponding Author: ORCID ID: https://orcid.org/0009-0000-5074-6650; Email: jgmundia@gmail.com

Article DOI: https://doi.org/10.37284/eajit.7.1.2212

Date Published:

15 September 2024

Keywords:

Mobile Network, Fraud, Concept Drift, Regulators, Service Providers, Focus Groups.

ABSTRACT

Background: Mobile network technology has exponentially advanced in the last decade and with this development, fraud activities have risen in equal measure resulting in companies and customers losing huge amounts of money as a result of, especially in developing economies that lag in the regulatory frameworks when it comes to Mobile network fraud. The purpose of the study was to explore Mobile network fraud in Kenya identifying the most common types of fraud, ways which service providers and regulators are employing to prevent or reduce fraud, methods currently used to detect fraud, and gaps thereof. Finally, the effect of concept drift in the automated fraud detection process. **Method**: A qualitative research method was adopted for the study and using a semi-structured question guide, four focus group discussions composed of 23 participants were conducted. The criteria used for selecting and placing participants into focus groups considered the following: The expert area of the participant, years of experience in the fraud ecosystem of the participant, and the organization to which the participant is attached. The availability and willingness of the participants were also considered in the selection process. The focus group approach was selected as it facilitated balanced discussion amongst all the players in the Kenyan fraud ecosystem, harnessing the power of group dynamics as it involved the regulators and the service providers who were drawn from different organizations. **Results**: The mobile network fraud ecosystem was stratified into three dimensions namely Fraud prevention which looked at the policies and methods used by both regulators and service providers to reduce fraud, Fraud categorization which aimed at categorizing different types of mobile frauds, and finally the Fraud detection which looked at the current tools being used to detect fraud. From the study, it emerged that although the regulators have provided strict guidelines on the customer onboarding process, not all service providers are currently using biometric approaches while onboarding new customers as this was highlighted as the entry point of most fraud cases. The study established five major types of Mobile network fraud in Kenya: SIM swap, SIM boxing, Wangiri, Commission arbitrage, and Hoax SMS and scams. Most of this fraud is committed using either SMS or voice channels; in some cases, both channels are used. Different matrixes derived from multiple factors are used by service providers while evaluating the criticality of fraud cases though not enforced by the regulators. The study also revealed that most of the fraud detection

Article DOI: https://doi.org/10.37284/eajit.7.1.2212

processes amongst the service providers still use manual tools that constantly require human input. While some of the detection processes are automated, concept drift is a major challenge for automated classification models due to the constant evolution of fraud patterns. **Conclusion**: The study revealed gaps in Mobile Network fraud prevention processes in Kenya as service providers still use non-biometric customer validation processes that are open to forgery and exploitation. A strict customer onboarding process that is fully automated and integrated should be used to address this gap. In the fraud categorization, there is no clear universal categorization matrix to guide the service providers while assessing the criticality of fraud and in this regard, a qualitative scientific model should be developed and used by all the stakeholders as a reference point. When it comes to fraud detection, concept drift is a major challenge, and service providers in Kenya still rely on manual processes due to the dynamic nature of mobile fraud. This exposes a huge gap in the detection process and there is a need to address this by developing systems and processes that will automatically detect and react to concept drift while automating the detection processes.

APA CITATION

Mundia, J., Miriti, E. K., Mburu, S., Kahonge, A. M. & Chepken, C. K. (2024). Assessing Mobile Network Fraud Threats and Prevention Strategies in Kenya. *East African Journal of Information Technology*, *7*(1), 279-300. https://doi.org/10.37284/eajit.7.1.2212

CHICAGO CITATION

Mundia, James, Evans Kirimi Miriti, Stephen Mburu, Andrew Mwaura Kahonge and Christopher Kipchumba Chepken. 2024. "Assessing Mobile Network Fraud Threats and Prevention Strategies in Kenya". *East African Journal of Information Technology* 7 (1), 279-300. https://doi.org/10.37284/eajit.7.1.2212.

HARVARD CITATION

Mundia, J., Miriti, E. K., Mburu, S., Kahonge, A. M. & Chepken, C. K. (2024) "Assessing Mobile Network Fraud Threats and Prevention Strategies in Kenya", *East African Journal of Information Technology*, 7(1), pp. 279-300. doi: 10.37284/eajit.7.1.2212.

IEEE CITATION

J. Mundia, E. K. Miriti, S. Mburu, A. M. Kahonge & C. K. Chepken "Assessing Mobile Network Fraud Threats and Prevention Strategies in Kenya.", *EAJIT*, vol. 7, no. 1, pp. 279-300, Sep. 2024.

MLA CITATION

Mundia, James, Evans Kirimi Miriti, Stephen Mburu, Andrew Mwaura Kahonge & Christopher Kipchumba Chepken "Assessing Mobile Network Fraud Threats and Prevention Strategies in Kenya.". *East African Journal of Information Technology*, Vol. 7, no. 1, Sep. 2024, pp. 279-300, doi:10.37284/eajit.7.1.2212.

INTRODUCTION

With the advancing Mobile network technology, fraud activities have risen exponentially resulting in companies losing huge amounts of money that ultimately cause severe financial damages (ZhiYuan, 2020). Mobile operators running mobile money platforms are well aware of the risks these platforms are exposed to – particularly the risk of fraud which can lead to the loss of two key commercial assets: reputation and revenue (Ogwueleka, 2009).

In Kenya, 71% of Kenyans have been a victim of mobile network fraud with SIM-swap accounting for the biggest share of these fraudulent activities. In a study carried out by the Communication Authority of Kenya (CAK), 46% of mobile fraud goes unreported and 64% of victims don't get their money back (CAK, 2019). With this number of fraud activities in Kenya, advanced fraud detection and prevention tactics must be developed. According to (Muriuki, 2017), Mobile network fraud specifically in Kenya was rooted in identity theft accounting for more than 80% of fraud in 2017.

According to Muriuki (2017), identity theft was the main driver of mobile network fraud in Kenya and he concluded that the introduction of biometric identification while registering and managing mobile network customers would eliminate most of the mobile network frauds. To

Article DOI: https://doi.org/10.37284/eajit.7.1.2212

the contrary mobile network fraud is on the rise despite some of the service providers adopting biometric identification. This is a result of the constant evolution in the fraud techniques applied by fraudsters. Concept drift which can be described as changes in the conditional distribution of the target variable which is also referred to as output given the input features or the inputs, while the distribution of the inputs may still stay unchanged (Gama et al., 2013) has been one of the challenges while dealing with the mobile network fraud detection. This means that a set of attributes that at one time indicated a non-fraudulent activity, can at a different time be a fraudulent activity. The effect of concept drift is Poor performance and reduced accuracy of the automated mobile fraud detection methodologies (ZhiYuan, 2020). Our research was aimed at trying to understand the mobile network fraud landscape and the effect of concept drift in the detection of fraud from both the perspective of the regulators and service providers who develop and implement fraud detection techniques and processes.

Background

Over the years there has been a tremendous evolution of the Mobile network infrastructure and the capability/services that can be delivered by the network. In the last 20 years, the Mobile network infrastructure has evolved from merely a (GSM) Global System for Mobile Communications platform for making calls and transmitting SMS (short message service) from one handset to another to a complex platform hosting and carrying multiple services. Recently, the Mobile network has become the backbone of the Mobile Money platform with the likes of Mpesa (Kenya), E-commerce platforms, E-delivery platforms, E-Taxi platforms, etc. With this development, the data generation dynamics, Velocity, and variety of data have exponentially increased. In this regard, fraud activities have also evolved into a complex web of touchpoints involving huge data sets. In addition, the fraud activity patterns have become unpredictable hence the need to adopt better ways to address these evolving fraud activities (Yang et al., 2018).

Although mobile cellular networks have become sophisticated and more developed in terms of fraud resilience, telecom carriers are still being impacted by fraud, especially in developing countries such as Kenya. Companies across the globe lose a huge amount of their revenue due to fraudulent activities (Tarmazakov et al, 2018). According to ZhiYuan (2020), In addition to mobile users incurring heavy losses, telecommunication companies exhibit a loss of over 7% of their revenue as a result of fraudulent activities and this number is even higher in developing countries and this figure excludes the reputation impact as a result of fraud. In Kenya, 71% of Kenyans have been a victim of mobile network fraud with 46% of mobile fraud going unreported and 64% of victims don't get their money back (CAK, 2019).

With this number of fraud activities globally and practically in Kenya, advanced fraud prevention and detection tactics must be developed. Although there have been positive developments when it comes to fraud detection, in the form of new sophisticated fraud detection algorithms (Sumaya et al.,2021) fraudsters have now developed new socially engineered tactics to access customers' data and use it to commit fraud.

Mobile Fraud Techniques

The following is an in-depth review of some of the Mobile network frauds in Kenya and how they are carried out.

SIMboxing

SIMboxing also known as bypass fraud is a form of fraud where international calls are diverted to a cellular device through the internet and the connections are routed back into the network as local calls resulting in a revenue leakage (Kala, 2021). SIMBoxing fraud occurs when the legal interconnect gateways are bypassed by fraudsters resulting in the diversion of traffic to illegal interconnect gateways (Nassir, 2020). This leads to a loss of revenue by the service provider and

Article DOI: https://doi.org/10.37284/eajit.7.1.2212

also poses a security threat as terrorists and other fraudsters can utilize this bypass to commit crimes as the call path is hard to trace. SIMBoxing is considered illegal in Kenya since the mobile network regulator does not license independent interconnect operators that are not full-fledged telecommunication service provides

SIMBoxing fraud is carried out using a device known as a SIMBox (Kala, 2021) shown in Fig. 1 which forms a part of a VoIP gateway installation. The function of a SIMBox is to hold numerous SIM cards linked to a gateway which is hosted separately from it. One SIM box can hold multiple mobile operators' SIM cards allowing it to operate with multiple GSM gateways hosted in different places. The operator of the SIMBox device can route or divert international calls made through the VoIP connection making the call connect as local traffic. This allows him to bypass international rates which are often high hence undercutting prices that would be charged by local mobile network operators who connect VoIP calls to the GSM voice network. The result of this is, an international call delivered at a subsidized rate meant for a local call. Apart from creating a revenue leak for the telecommunication companies, it also hurts the quality, availability, and reliability of service for legitimate customers as large volumes of calls are injected causing bandwidth restrictions which in turn compounds the revenue loss to the mobile network operators

Figure 1: SIMBox Device

Figure 2 illustrates an international call path following a legitimate Regulated Interconnect and *Figure 3* illustrates a SIMboxed call that has been diverted and routed to appear as a local call.

Figure 2: Legitimate call path

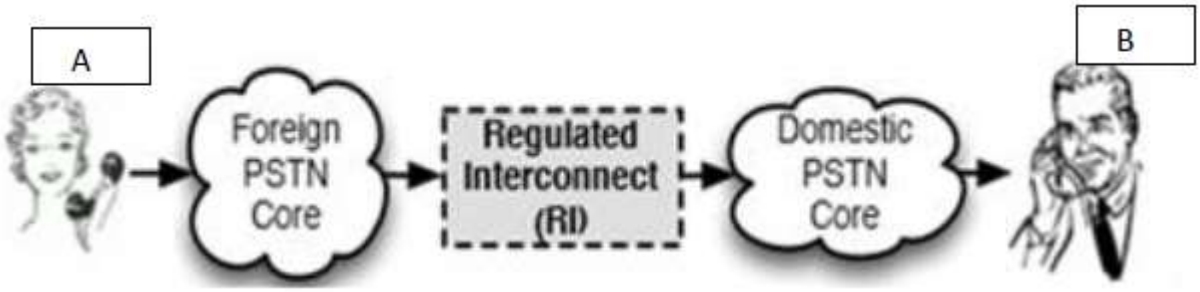
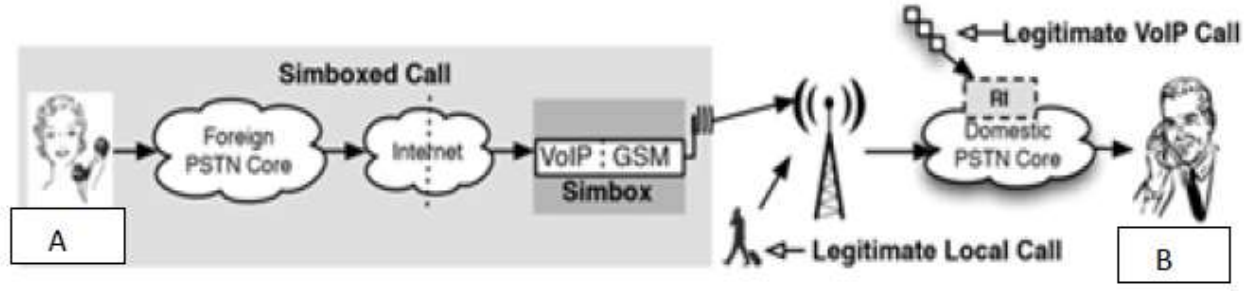


Figure 3: SIMBoxed call path



Article DOI: https://doi.org/10.37284/eajit.7.1.2212

Wangiri

Wangiri, which is derived from the Japanese "one ring and cut"; wan means "one" and giri means "hang up" is a scam in the International Revenue Share Fraud (IRSF) schemes (Mais et al., 2018). Wangiri fraud occurs when fraudsters call a targeted list of numbers randomly and hang up before the subscriber answers the call. The originating number is an International Premium Rate Number (IPRN) and when the subscriber calls back as prompted by the missed call, he is encouraged to remain on call by the use of an answering machine that utilizes messages that are prerecorded promising the subscriber rewards. The result of this is huge international billable time which is paid by the unaware subscriber with the fraudster pocketing this revenue. *Figure 4* below illustrates how the Wangiri scam is committed when targeting a specific tele-network resulting in fraudsters generating revenue from it (Jessica, 2018)

Figure 4: Wangiri scam

SIM swaps:

A SIM (Subscriber Identity Module) card is a physical or virtual component of every mobile device in a GSM network that provides a unique identity on mobile devices (Snehal et al., 2019).

SIM Swap fraud (Roger, 2023) occurs when a criminal or fraudster replaces or clones the SIM card from a victim's mobile device and gains partial or full control. SIM Swaps attacks can broadly be classified into three categories depending on how they are initiated

- Physical SIM Swap Attack: This occurs when the fraudster gains physical access to the mobile device and control of the SIM card by either using the same mobile device or swapping the card to a different mobile device.
- Insider SIM Swap Attacks: This occurs when an employee within the mobile service provider who has access to the internal systems orchestrates the SIM swap. This can be carried out by him/her sharing information or by personally performing the SIM swap.
- Socially Engineered SIM Swap Attacks: This occurs when the fraudster gains necessary information from the victim to perform a SIM swap by the use of social engineering tactics. This can also occur when the fraudster uses social engineering tactics to manipulate the service

Commission arbitrage:

According to Philip (2015), arbitrage is the practice of taking advantage of differences in markets or conditions of a product to make a profit. Commission arbitrage is whereby telecommunication dealers and agents take advantage of the commissions given by the service providers once a service is provided to customers.

Commission arbitrage fraud occurs when the dealer or agents collude with customers in

Article DOI: https://doi.org/10.37284/eajit.7.1.2212

manipulating the number of transactions due for commissioning by the service provider leading to the telecommunication companies paying huge sums of money as commissions to the dealers and agents. This fraud is categorized into two main classes

- Split transactions: In this kind of fraud, the agent or the dealer advises the customer to split one transaction into many small transactions hence maximizing the number of transactions that are eligible for commissions. Below is an example of this kind of fraud, A customer wants to perform Mpesa deposit of KSH 100,000 but instead of performing this transaction in one go, the agent or the dealer splits this into 100 transactions of KSH 1,000 each hence receiving commissions of the extra 99 transactions and the same applies for deposits and transfers. In cases where there is transaction fee involved; the fraudulent agent will try to optimize the commissions Vis-à-Vis the cost of performing the transactions hence leading to a major revenue leakage from the service providers.

- Recursive transactions: In this kind of fraud, the fraudulent agent or dealer uses a certain amount of money to create transactions which are subject to commissioning. The agent will transfer the amount from one account to another multiple times taking advantage of the subsidized or zero-rated transactions to create fictitious commissionable transactions an example of this kind of fraud is whereby a dealer or agent deposits KSH 20,000 to one of his bank accounts linked to Mpesa account, withdraws it from Mpesa account and repeats this cycle hundreds of times and in some cases using different accounts. This in turn creates a huge number of commissionable transactions for the dealer or agent leading to huge revenue leakages from the service provider

Hoax SMS and scams:

A message is transmitted digitally in a GSM network without using the internet service via the short messaging service (SMS), which has become one of the most utilized communication services due to its ease of use and the minimal costs incurred while using the service (Biju, 2022). The popularity of SMS service is also boosted by the fact that it does not require internet services to operate making it popular for both the smart phone users as well as the non-smart phone users. Due to this increase in the use of SMS, fraud cases using this media are also on the rise with the fraudsters spending little effort and cost to reach thousands of subscribers. This form of fraud can be categorized into two broad categories.

- Targeted SMS: This kind of fraud targets a specific person or group of people intending to extort money from them. In this kind of fraud, the fraudsters will have prior knowledge of the targeted population which includes their phone numbers. An example of this kind of fraud is when a fraudster gets hold of the phone numbers of all employees of a particular company and sends an SMS to all the employees requesting some contribution of funds towards a specific project or course. These SMSs are usually customized to the specific audience to look and feel authentic.

- Random SMS: This kind of fraud does not have a specific group of people as the target. The fraudster will send a more generalized SMS to thousands or even millions of subscribers with the aim of either extorting money or information from them. In most cases when the subscriber returns the SMS with information, the fraudster might use this information to further commit a targeted fraud using the information given. An example of this kind of fraud is when a fraudster sends an SMS to thousands of subscribers informing them that they have won some price in a particular promotion and requests information from the subscriber so that they can have their price processed or in some cases send money to a particular number to ‘unlock’ the price.

Objectives

Article DOI: https://doi.org/10.37284/eajit.7.1.2212

The main objective of the research was to Characterize mobile network fraud and the effect of concept drift in Mobile network fraud detection with respect to prediction accuracy.

The specific objectives were to:

- Determine steps adopted to prevent or reduce Mobile network fraud
- Determine the common types of mobile network fraud in Kenya.
- Determine what channels by which mobile network fraud is initiated and propagated.
- Identify how concept drift affects the fraud detection process and identify the factors that contribute to the concept drift while using automated fraud detection techniques.

Research Questions

Based on the research objectives, below are the research questions that we tried to answer

- What preventive measures are adopted to reduce Mobile network fraud in Kenya?
- What are the common types of mobile network fraud in Kenya?
- What channels by which mobile network fraud is initiated?
- How does concept drift affect the prediction accuracy while using automated fraud detection tools and what are the contributing factors?

Methodology

The focus group technique was applied as the primary data collection method for the qualitative research in the exploration of the common mobile network fraud in Kenya and the effects of concept drift while using automated fraud detection tools.

The main justification for the adoption of the focus groups in this research was that when investigating complex behaviors and motivations, the outcome of the interaction in focus groups also known as “the group effect” (Carey, 1994) was very key in understanding the current Mobile network fraud ecosystem and the effects of concept drift while using the automated fraud detection tools. In addition, specific kinds of interactions that occurred offered valuable data for the study culminating in consensus and diversity among the participants.

Participants

In the study, a total of 4 focus groups were formed comprising between 5 and 7 participants. To ensure adequate diversity of opinion, participants from different expert areas that are involved in the Mobile network fraud were involved. The composition of the focus group also took into consideration the market share controlled by each service provider as per data collected by CAK (2023). In addition, more than one session was carried out with some of the participants to clarify or shed more light on certain issues that were raised during the group discussions.

Table 1 below represents the participants who took part in the study. The criteria for inclusion in the focus group included: - The expert area of the participant, years of experience in the expert area, and the organization to which the participant is currently attached. This ensured that all the mobile service providers in Kenya were represented in the study. The following were expert groups involved in the study as they formed a complete ecosystem of Mobile fraud detection and regulation in Kenya.

Fraud Analysts from the service providers: - This is the team responsible for analyzing all the fraud cases in a service provider environment, they receive the calls from the customers and analyze the impacts of each fraud case that is reported

Fraud Algorithm developers: - This is the team in the service provider that is responsible for the development of machine learning models and algorithms and then deploys them to automate the fraud detection process.

Fraud and compliance team: - This is the team that develops and enforces the requirements concerning fraud as per the regulators’ policies. .

Article DOI: https://doi.org/10.37284/eajit.7.1.2212

They also constantly communicate with the regulators to update the policies if the need arises.

Mobile Money Fraud Regulators: - This is the team from the regulator side whose primary role is to draft laws and policies that define what fraud is and their respective thresholds. They also monitor the service providers for the bleach of the fraud regulations.

Fraud Algorithms Architect: - This team can be drawn from both the service providers and also regulators whose primary role is to design fraud algorithms used to classify fraud per the set laws and policies by the regulators

Table 1: Focus groups participants

Participant #	Participant Code	Focus Group #	Area of expert	Years Of experience	Organization
P1	FAA1	F1	Fraud Analyst	8	Service provider A
P2	FAB1	F1	Fraud Analyst	11	Service provider B
P3	FD1	F1	Fraud Algorithms developer	9	Service provider B
P4	FLA1	F1	Fraud and compliance lead	13	Service provider A
P5	MNL1	F1	Fraud Analyst and policy	3	Mobile Network Regulator
P6	MML1	F1	Fraud Analyst and policy	7	Mobile Money regulator
P7	FRA1	F1	Fraud Algorithms Architect	11	Service provider C
P8	FAC2	F2	Fraud Analyst	4	Service provider C
P9	FAB2	F2	Fraud Analyst	3	Service provider B
P10	FD2	F2	Fraud Algorithms developer	4	Service provider A
P11	FLB2	F2	Fraud and compliance lead	12	Service provider B
P12	MNR2	F2	Fraud Analyst and policy	10	Mobile Network regulator
P13	MMR2	F2	Fraud Analyst and policy	3	Mobile Money regulator
P14	FAA3	F3	Fraud Analyst	5	Service provider A
P15	FD3	F3	Fraud Algorithms developer	7	Service provider C
P16	FLC3	F3	Fraud and compliance lead	16	Service provider C
P17	MNR3	F3	Fraud Analyst and policy	14	Mobile Network regulator
P18	FRC3	F3	Fraud Algorithms Architect	17	Consultant
P19	FAA4	F4	Fraud Analyst	5	Service provider A
P20	FAB4	F4	Fraud Analyst	5	Service provider B
P21	FD4	F4	Fraud Algorithms developer	6	Service provider A
P22	MNR3	F4	Mobile network Fraud Regulator	9	Mobile Network regulator
P23	FRC4	F4	Fraud Algorithms Architect	3	Service provider C

Article DOI: https://doi.org/10.37284/eajit.7.1.2212

Procedure

Focus groups were carried out until saturation of new information was attained with a follow-up meeting done to clarify any issue highlighted by the moderator during the focus group discussions. The sample size was not predetermined before the focus group to avoid missing out on any crucial information. The facilitator ensured that each of the participants was given enough time to express their opinion and any additional comment above the scripted questions was highly recommended to ensure that the facilitator collected as much information as possible from the participants. The facilitator did not act as an expert in the area of mobile network fraud but rather guided and facilitated the discussion in the below areas

- Steps adopted to prevent or reduce Mobile network fraud
- Common types of mobile network fraud.
- Channels by which mobile fraud is initiated and propagated
- Effects of concept drift while detecting mobile network fraud using automated tools

The following is a summarized process that was followed while running the focus groups which were all conducted online: -

Invitations were emailed to the participants who matched the selection criteria, highlighting the intention and purpose of the research and the role they would play.

Once the participants accepted the request, they were initially divided into 3 groups depending on their expert area and the organization they were affricate to, this was to ensure that each of the focus groups was well represented and balanced.

Google Meet was used to schedule and conduct the meetings for all focus groups.

Before the meetings the researcher and the moderator met and agreed on the role, purpose, and how the meeting would be conducted and the moderator was only to moderate the sessions and ask follow-up questions if needed.

Once all or a critical number of the participants was met, 4 participants were considered as the critical number based on the considered literature (Krueger, 1997), the moderator started the meeting by introducing himself and the researcher and allowed all the participants to introduce themselves.

The participants were requested to ask any questions about the research area, data sharing, or any other questions before the main discussion commenced.

The moderator then started the introductory questions and based on the alphabetical order of the participants; they gave their introductory remarks.

Once the introductory remarks were completed the meeting officially started and the predefined questionnaire was used as a guide

The moderator tracked and recorded the answers and asked follow-up questions if the area was unclear.

At the end of the discussions, the participants were requested to ask any follow-up questions or comments before the meeting closure.

The meetings were closed with a vote of thanks from the moderator.

Once the meeting ended the results were coded for analysis and if some clarifications were required, a follow-up meeting with the participant was scheduled.

This process was repeated in the subsequent meetings and adjustments of time taken per question, the follow-up questions, and the discussion flow were made in the subsequent meeting as a result of the learnings from the previous meetings.

After the initial first 3 focus groups, additional participants were enrolled to participate in the 4th focus group.

Focus group discussion lasted between 1.5 to 2 hours and was verbatim scripted for later analysis.

Article DOI: https://doi.org/10.37284/eajit.7.1.2212

Group dynamics handling:

The moderator ensured that no participant felt their point was not considered by allowing them to finish their contributions without intercepting them.

Other group members were allowed to comment, ask the participant questions, agree or even disagree with them but any discussions outside the scope of the study area were not allowed.

Where different opinions were given for a particular issue, the moderator recorded all the responses without discarding any participants' answers and this was handled during the analysis phase.

In case of conflict and different opinions on a specific issue an informal voting was done to assess the majority view and if there was a tie on the issue, the moderator highlighted this and was recorded during analysis and a follow-up meeting with the participants was done to get clarity on the issue if required.

When a topic lasted for more than 15 min the moderator interjected so that more time was not consumed on one topic

Change of mind by a participant as a result of other participants' contributions was encouraged and noted.

Participants confidentiality

Participants' anonymity and confidentiality were persevered by applying the following: -

Participants were not allowed to mention the name of the organization they were affiliated with during the discussions and were only allowed to disclose their years of experience and the expert area.

The participants were labeled by a code name given before the meeting and this was maintained during the group sessions, the real names of the participants were not used anywhere during the group discussions.

Question guide

Based on the recommendation by Krueger (1997) on the focus group methodology, a semi-structured question guide (See *Table 2*) was developed to act as a guide during the group discussion. After in-depth collaboration with an expert on focus groups and input from the literature review (Krueger, 1997), the questions were developed. The question guide included introductory or opening questions which allowed the participants to get well acquainted with the process and also feel comfortable among other group members. Then transition questions were introduced to open up the key discussions for the study. During the discussion, the moderator encouraged follow-up questions that were not necessarily in the question guide to allow the gathering of more data that would be useful for the study. The moderator also avoided guiding the participants in a particular direction as it would distort the information shared and he also limited interpretations while the participant was talking.

Article DOI: https://doi.org/10.37284/eajit.7.1.2212

Table 2: Question guide

Q #	Question	Background information	Research Question 1 (**What are the common types of mobile network fraud in Kenya?**)	Research Question 2 (**What channels by which mobile network fraud is initiated?**)	Research Question 3 (**Is concept drift a major concern with the currently used fraud detection tool?**)	Research Question 4(**What factors contribute to concept drift in mobile fraud detection?**)
1	Is Mobile network fraud a major challenge in the organization?	X				
2	Is there a policy that guides the fraud threshold	X				
3	How is customer registration carried out Follow-up question: What are the precautional measures taken to ensure the authenticity of the customer?	X				
4	What are the most common types of fraud that you register?		X			
5	What are the parameters used to rate and categorize types of fraud?		X			
6	What is the most affected population by mobile network fraud? Follow-up question: Does the education level or social status of an individual correlate to the probability of being frauded?		X			
7	what channel by which fraud is initiated?			X		
8	what channel by which fraud is carried out?			X		
9	Are most frauds targeted to a particular individual or it is random?			X		

Article DOI: https://doi.org/10.37284/eajit.7.1.2212

10	Is the fraud detection automated in the organization?	X		
11	Is there concept drift identified during the fraud detection process? How?	X		
12	Does the issue of concept drift significantly affect the detection accuracy? How?	X		
13	What are the most common types of concept drift?	X		
14	What contributes to the concept drift?			X
15	Are there tools currently being used to detect drift? Which ones?			X
16	Is there a need to automate the drift detection and rectification?			X

Article DOI: https://doi.org/10.37284/eajit.7.1.2212

Data analysis:

The collected data was analyzed and evaluated using the thematic analysis methodology (Braun et al., 2006). The recorded discussions were codified into various themes by the use of preset criteria. The criteria were based on the literature (Braun et al., 2006) and then used as codes to aggregate the transcript of the discussions Nvivo and Windows Media Player were the software used to transcribe the recorded discussions. Using the inductive thematic approach (Silverman, 2005) the coded data was analyzed for the recurrent instances in the data set and then grouped to form a general concept or sub categories which then gravitated to form main categories.

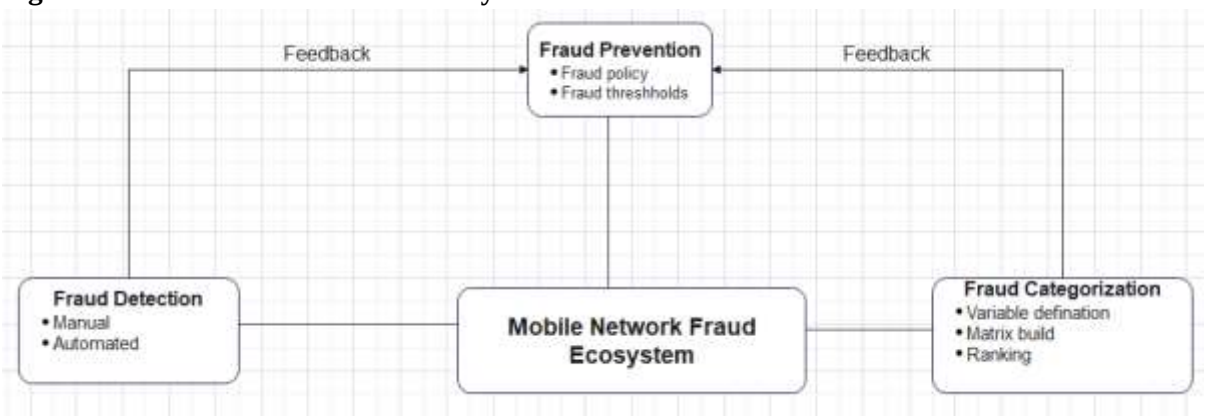
The facilitator also took into consideration the participant's expertise and years of experience, the context in which comments or responses were made, the influence of other participants in the group, and also participant's encounters and experiences. These factors provided an auxiliary dataset that was put into consideration. In addition, views and opinions that mutated as a result of group dynamics and the opinions of groups expressed as a result of consensus were highlighted.

Results:

The data saturation point was attained after the fourth focus group session in the study. A total of 23 participants drawn from different expert areas in the line of mobile fraud detection ecosystem were involved in the study and were grouped into 4 focus groups. The group composition was such that different expert areas from different organizations were represented in each group enhancing group interactions amongst different organizations and expert areas representations. The mean of the years of experience of the participants was 8 years, with a maximum of 17 years and a minimum of 3 years. This was a key consideration in our study as it ensured that the participants had vast knowledge and experience in the area of study.

A framework describing the mobile network fraud ecosystem was extracted and organized along the following three dimensions which were defined before the study: - Prevention, categorization, and detection. Details for each dimension were then extracted from the transcripts.

Figure 5: Mobile Network Fraud Ecosystem



Mobile Fraud Prevention

In this dimension the study aimed to understand whether the service providers considered mobile fraud as a major issue while running their business and also understand whether there were fraud thresholds that have been set by the policymakers to guide the service providers on what is considered fraud from a regulatory perspective. The study also aimed to understand whether there were precautionary measures taken by service providers to prevent fraud.

From the study, all the service providers considered mobile network fraud as a major issue and had developed clear policies on how they deal with fraud. From the responses amongst all the groups, they all unanimously agreed that this was

Article DOI: https://doi.org/10.37284/eajit.7.1.2212

a major concern to the industry as a whole, and policies governing mobile network fraud were in place to monitor and provide guidelines on mobile network fraud.

> *"Fraud has been the biggest threat to our existence as a telecommunication company because one major fraud incident can bring down the organization"* (FAB1)

> *"As a company, we lose billions of shillings due to fraud and sometimes we decide not to publicly report these numbers as it may lead to more catastrophic reputation damages, I also think fraud cases are happening now that we are not aware of"* (FAA3)

The mobile network regulators also provided regulations and guidelines that define what mobile fraud is and the thresholds that need to be met for a transaction to be considered fraudulent. All the service providers employed some form of user identification during the customer registration process which is considered as the entry point of service provider customer interaction. Although biometric customer registration is not enforced by regulators while registering new customers, some of the service providers have deployed it as the primary method of customer identification. Other service providers still use Identification cards as the primary identification method.

> *"As the regulators, our primary role is to protect the consumers from losses and that is why we have developed frameworks to guide the telecommunication companies when it comes to fraud, we also follow up to make sure these policies are strictly followed so as to protect the consumers"* (MNR3)

In terms of customer onboarding policy, the Communication Authority of Kenya (CAK) and Central Bank of Kenya (CBK) which are the regulators have provided guidelines on how a customer or subscriber should be registered and the documents to be provided. They have also provided guidelines to confirm whether the details provided by the customer are authentic or not by integrating the customer registration process with the government's database of persons. Two major concerns of this process are that the process is not real-time and the actual verification happens days after the customer has already been registered. The other issue identified with the registration process is that biometric data was scantly used with most of the service providers admitting that they don't use it as it is not compulsory from the regulation point of view which creates a loophole where fraudsters can register themselves with the service provider using stolen or illegally obtained documents.

> *"Yes, the regulators require us as service providers to know our customers before registering them but when a customer brings fake identification while performing the registration process, we have no mechanism to know, we are not the police to investigate how genuine the documents are"* (FAA4)

The lack of an updated database of persons by the government is a key stumbling block in the process of fully using biometrics during the customer registration process as service providers fully rely on this data to match the identity of the customer and his bio (fingerprints and facial images). As a result of this most of the service providers opt for a manual verification process which is prone to forgery and impersonation.

> *"The government system that we are meant to connect to and verify the name and the ID number of a potential customer is always down and inaccessible and it can stay for days like this, so we are forced to use manual processes"* (FLC3)

> *"Sometimes we cannot use biometrics for the registration in the remote villages where there is no power to run these systems"* (FLB2)

Mobile Fraud categorization

In this dimension of the study, the aim was to understand what parameters service providers and regulators used to categorize or measure the severity of fraud cases. This was critical as it enabled us to understand what are the most catastrophic kinds of Mobile network fraud from

Article DOI: https://doi.org/10.37284/eajit.7.1.2212

both the regulators' service providers' perspectives.

From the study, it was established that all the service providers use a matrix that consists of the following variables to assist in the fraud assessment: - Customer's financial Impact, Service Provider's financial impact, number of customers affected, organization reputation, and political impact of a fraud incident. The weights allocated to variables varied from one service provider to another. Mobile network regulators weighted customer financial impact and the number of customers affected by a fraud instance as the highest. One service provider adopted the regulator's weighed evaluation matrix while the others adopted a different evaluation matrix as the regulator just offered a guideline and didn't force service providers to adopt its evaluation matrix. One of the service providers weighted the Service provider's financial losses as the highest. Though the political impact was considered as a variable or criteria to measure fraud impact, all the service providers weighted it the least.

> *"As the regulators, our main focus it the consumers so any fraud affecting the consumers will rank the highest in our ranking."* (MNR3)
>
> *From the telecommunication perspective, though we really care for our customers, our main objective is to make money and if a fraud affects our books, then that will rank highest, unwritten rules"* (FLB2)

The other question that the study was to answer is the population by which most of the fraud targeted. This question was tied with another question that wished to address whether most mobile network fraud is just random or targeted. All the service providers had different views on these questions with some arguing that most successful fraud cases happened to the less informed population of the society while other service providers argued that fraud was random. From the discussion of the focus groups, it was concluded that whether the fraud was random or targeted, the less informed, less educated members of the society accounted for the most successful fraud cases and there was a high correlation between the probability of being frauded and the social status of the customer. There were however some exceptions to these findings where some fraudsters target the high members of society with a case example provided by one service provider that targeted members of parliament with about a 50% success rate although this population is considered to have higher social status.

> *"From my experience fraud is random what happens after the initial contact with the fraudsters is what determines the direction of the fraud"* (FAC2)
>
> *"Some frauds are targeted whereby the fraudsters have very detailed information about their targeted victim which they use to commit the crime."* (MNR2)
>
> *"From our experience, mobile fraud has both the dimensions as targeted or random but the success of the fraud mostly depends on the victim's actions after the first encounter"* (FAC2)

From the focused groups, there was a consensus amongst the participants from both the regulators and the service providers that there are five common mobile network frauds in Kenya namely: Sim swap, SIMboxing, Wangiri, Commission arbitrage, and Hoax SMS and scams which are extensively discussed in the literature review session. In the study, a severity ranking on the types of frauds was carried out basing the ranking on different attributes that are used by the service providers and the regulators to determine the criticality and frequency of a fraud type. *Table 3* represents the ranking based on the ranking attribute

Article DOI: https://doi.org/10.37284/eajit.7.1.2212

Table 3: Fraud Type Ranking

Rank	Customer financial Impact	Service Provider financial impact	Customers affected	Political impact	Organization reputation
1	Sim swap	Simboxing	Hoax SMS and scams	Hoax SMS and scams	Sim swap
2	Hoax SMS and scams	Commission arbitrage	Sim swap	Sim swap	Hoax SMS and scams
3	Wangiri	Sim swap	Wangiri	Wangiri	Simboxing
4	Commission arbitrage	Wangiri	Commission arbitrage	Commission arbitrage	Commission arbitrage
5	Simboxing	Hoax SMS and scams	Simboxing	Simboxing	Wangiri

Customer financial Impact

This variable measured the customers' financial effect of fraud. From the group discussions, it was consented that Sim swap fraud accounted for the highest financial losses from the customers' perspective followed by Hoax SMS and scams, Wangiri in that order. Simboxing had very little financial impact on the customers. The highest-ranked fraud in this variable directly targeted the customers.

> *"Sim Swap fraud directly affects the customers who are also the primary losers in this kind of fraud, when the lens used to measure the impact of fraud is set to the impact on customer, Sim swap and Hoax SMS will rank the highest"* (FAA3)

> *"Sim swap followed by Hoax SMS will rank the highest when it comes to the impact on the customer as the commutative money lost by the customers as a result of these frauds is the highest"* (FLC3)

Service provider Financial Impact

Under this variable, the fraud type that inflicted the highest financial loss from the service providers' perspective was ranked with Simboxing and Commission arbitrage being ranked the highest as the service providers were the primary losers in this kind of fraud. Wangiri and Hoax SMS seem not to have a huge financial loss from the service provider perspective.

> *"Simboxing and Commission arbitrage is fraud committed by customers toward the service provider resulting to huge financial losses by the service providers in which case there are the sole losers as a result of this fraud."* (FLA1)

Customers affected

This variable is aimed to measure which type of fraud affected the highest number of customers regardless of the amount involved. Using this variable Hoax SMS, SIM swaps, and Wangiri were ranked the highest in that order with SIMboxing and Commission arbitrage ranking the lowest.

> *"Hoax SMS affects most of the customers as the fraudsters use automated machines to send huge numbers of SMS at once to customers. Customers numbers can randomly be generated using very simple algorithms and then hoax SMS sent to them hence the reason why they affect a huge number of customers"* (FAA4)

Political impact

This variable is used to assess how a particular fraud alters the political dynamics of the country and under this variable Hoax SMS was ranked highest as fraudsters can utilize this fraud to pedal a specific political narrative, SIM swap was ranked 2nd under this variable as fraudsters can perform swaps of politically influential members of the society SIM cards and use them to originate a politically motivated communication.

> *"Kenya being a very politically active country, the mobile network can be used as a*

Article DOI: https://doi.org/10.37284/eajit.7.1.2212

media to propagate propaganda, cause panic and even deny service to member of the society so that is why this variable is used to measure what type of fraud has the highest likelihood to result to political polarization and in this case, hoax SMS tops the list" (FRA1)

Organization reputation

This variable assessed how fraud affects the reputation of the organization. SIM swap and Hoax SMS ranked the highest which means that this form of fraud can result in huge reputation damage to the organization.

> *"When customers lose money through fraud and they cannot recover it back because the service provider does not assist them, then customer loses confidence in that service provide and if this occurs to many customers using that service provider, then the reputation of that organization will be dented. In this regard, SIM swaps and Hoax SMS are the highest culprits."* (FAB2)

Additionally, under this dimension, the study wished to understand the channels by which mobile network fraud is initiated and also the channels by which fraud is propagated. All the focus groups consented that there are 2 major channels by which mobile fraud is initiated which are voice and Short Message Service (SMS). Though there are channels like emails, social media, and mobile applications, their impact is not yet significant as of today in Kenya according to both the service providers as well as regulators. In terms of fraud propagation, both voice and SMS dominated with the other channels having a small impact. It was recorded that mobile fraud could be initiated using one channel and be propagated using another channel which seems to be the most cases. One participant from the service provider reported that in most fraud cases of fraud, multiple channels are involved with the combination of SMS initiated and voice propagated being the most common.

> *"Most of the fraud cases are multi-channeled whereby multiple channels are utilized to initiate and ultimately commit fraud with voice calls and SMS driven fraud being the most common"* (FAB4)

> *"SMS and voice are the most common channels fraudsters use but why this is the case is that they are the most dominant mode of communication amongst the Kenya population, maybe in future other channels will emerge"* (FD3)

Mobile Fraud detection

This dimension in the study aimed to understand what tools are currently being used by the service providers to detect fraud and also understand whether there are policies in place to guide the detection tooling from the regulators. From all the service providers, the fraud detection process is partially automated. It is worth noting that the level of automation varies from one service provider to another with the most highly automated service provider having automated around 45% of the detection process with the lowest automated service provider standing at 35%.

> *"We have automated around 45% of our fraud detection processes but we plan to hit 60% by the end of 2027"* (FLA1)

> *"For now, we are still automating the processes that we use to detect fraud and I can say we are now at around 35% in the automation process."* (FLB2)

This finding means that most of the fraud detection process in Kenya's mobile network is manually done with the help of non-artificial intelligence (AI) driven tools are which means they semi-automated. Although there is no available best practice or industry standard level of automation, organizations that embrace automation of fraud detection processes ends up to be more efficient and effective in mobile fraud management (Aisha et al.,2016). All the focus groups consented that the major challenge with the automation process was due to the constant changes in the fraudsters' tactics and the available tools had to be manually adjusted to capture the

Article DOI: https://doi.org/10.37284/eajit.7.1.2212

evolved fraud patterns. This leads to some of the service providers resulting in manual processes which are very cumbersome and error-prone due to the number of subscribers and fraud cases involved.

It was consented by the participants that, concept drift is one the major challenges that service providers and regulators face when it comes to automation of fraud detection process as the models' accuracy significantly reduces with time resulting in erroneous classifications which can be both false positive or false negative. The service providers and the regulators indicated that there is currently no approach or methodology that is in use to address this challenge. They admitted that most of the fraud analysts will revert to manual processes once the detection models seem not to be accurate.

> *"The ever-evolving fraud tactics employed by the fraudsters make the automation process difficult as the current models that we use, do not automatically adapt to the new fraud activities and we are forced either to manually adjust them or result to manual processes"* (FRC3)

The study also desired to understand what type of concept drift was more prominent on the mobile network among the three drifts that is:

Real concept drift: - This is defined as the changes in the probability of y given X p(y|X). These changes can occur when p(X) changes or not.

Population drift: - This is defined as the change in population by which the future samples will be drawn as compared with the already drawn design/training sample (Geoffrey et al. 2016).

Virtual drift: - virtual drift has been defined (Tsymbal 2004), to be caused by a lack of complete data representation as opposed to a change in concepts in the real sense. Virtual drift aligns with the shift in data distribution resulting in a decision boundary shift.

From the focus group discussion, there was no conclusive consensus on the most common type of drift as the model developers from all the services provided had different opinions on this issue but they all agreed that all the types of drifts are indeed experienced while using the automated fraud detection process. In terms of the drift causes, both the Data Distribution Change and Input data change were involved in equal measure to cause concept drift. It was also consented that there are no tools available from the service providers to detect, mitigate, and correct concept drift in addition to the regulators having no defined policy to guide on this issue. As a result, even in the automated processes, management of the concept drifts is done manually through recalibration of the detection models.

Discussion:

To fulfill the aim of the study and to well understand the mobile network fraud ecosystem, a qualitative method of focus group was adopted. Focus group discussion enabled us to understand the topic from the practitioners' perspective giving room for deep discussions and iteration among all the different parties and expertise in the line of mobile network fraud. The discussions brought forward participants from the Mobile network regulators and service providers which allowed for a detailed introspective of policy formulation, prevention, categorization, and detection of Mobile network fraud. The group discussions also allowed the participants to give their real-life scenarios while dealing with Mobile network fraud which enriched the data collected for the study. Additionally, focus group discussion was opted for this qualitative study as it will act as a guide that can lead to future quantitative studies in this area, hence looking at the holistic Mobile network fraud ecosystem was paramount to aid future studies.

A theoretical framework describing the mobile network fraud ecosystem in Kenya was developed. The first pillar of the framework is *Fraud prevention* which describes ways in which mobile fraud is prevented. Two components are the building blocks of this pillar, i.e. *Fraud policy* and *Fraud thresholds*. Fraud policy defines what a fraudulent incident looks like while the fraud threshold identifies the minimum attributes of a

Article DOI: https://doi.org/10.37284/eajit.7.1.2212

transaction to qualify to be a fraudulent transaction. From the study, mobile network regulators in collaboration with the service providers define the fraud policies and thresholds that describe mobile network fraud. These policies and thresholds are reviewed and revised through continuous feedback from the other pillars.

The study revealed that mobile network fraud is constantly evolving and calibration of the fraud thresholds needs to be reviewed frequently to capture the new fraud patterns. Formulating fraud policies and thresholds therefore an infinite process that has to be reviewed and updated continually to maintain detection accuracy.

The second pillar of the framework is *Fraud categorization* which enables mobile network fraud to be ranked in severity based on selected criteria or variables. The building blocks of this pillar are *variable definition, matrix build*, and *ranking*. The variable definition determines the lens by which fraud criticality is evaluated. The matrix build enables a combination of variables with different weights to be used to evaluate the severity of mobile network fraud. The ranking is then done based on the variable or a set of variables to determine which is the most critical type of fraud.

The study categorized and ranked mobile fraud on the impact of the customer and the service provider. This was an enhancement from a study carried out by Rupa et al. (2015) which categorized cellular network fraud based only on the customers' experience and concluded that the measure of critically of mobile fraud should be the impact the fraud has on the customer. It emerged from the study that the impact the fraud has on the service provider is equally important in categorizing fraud cases. In the study, it was evident from the group discussions that some mobile network frauds are committed by the customers or agents towards the service provider a case example being Commission arbitrage and SIMboxing fraud in which case the service provider is the sole loser. The study also revealed that the matrix used to categorize fraud should constantly be revised by both the regulators and the service providers to properly categorize the new emerging fraud patterns.

The third pillar of the framework is *Fraud detection* which evaluates the fraud detection methods employed. The building blocks for this pillar are manual and automated. Under this pillar, the level of automation of the fraud detection process and the challenges that comes with the automation were evaluated.

In the study, it was revealed that service providers are still using manual processes to detect fraud cases as the development of the automated detection processes cannot keep up with the evolving fraud cases and there is a great need to evaluate this gap and develop more efficient solutions. It was also brought forward that concept drift as related to the automation of the fraud detection process remains one of the major challenges. This is compounded by the massive dataset that service providers deal with hence the need to come up with solutions to address this challenge is of paramount importance. When it comes to automated classification models, a feedback process can be incorporated (Gama et al., 2013) to capture the concept drift and action accordingly. In this regard, a comprehensive study can be carried out to evaluate the effectiveness of the feedback process as one of the approaches that can be adopted by the service providers to reduce the concept drift effects and improve the automated detection efficiency in the mobile network ecosystem.

Limitations

The assumption was that the research sample was a representation of the population and their input represented a holistic view of the population/environment in question.

Group dynamics might have affected participants' responses altering their true position on the issue in question.

As the discussions involved participants drawn from competing service providers and regulators, some critical information might have been held

Article DOI: https://doi.org/10.37284/eajit.7.1.2212

back by the participants to reduce their exposure to the regulators and also other competing service providers

As there was no quantitative data collected and analyzed, hence we cannot make very strict conclusions.

Conclusion

The study revealed that though the regulators have provided clear guidelines on fraud prevention procedures, especially during the customer onboarding process, most of the service providers don't fully adhere to them. A case example of this is that service providers still use non-biometric customer validation processes which are open to forgery and exploitation. This is a gap in Mobile Network fraud prevention processes in Kenya and can be addressed by regulators enforcing a strict customer onboarding process that is fully automated and integrated with the government's database of persons.

The study revealed the most common types of mobile fraud in Kenya today namely SIM swap, SIMboxing, Wangiri, Commission arbitrage, and finally Hoax SMS and scams. Based on different attributes the fraud types were also ranked. This insight would allow the service providers and regulators to know what kind of fraud type to focus on. In the fraud categorization, there is a gap in that there is no clear universal categorization matrix to guide the service providers while assessing the criticality of fraud and in this regard, a qualitative scientific model should be developed and used by all the stakeholders as a reference point. We also propose that a quantitative study be done to scientifically evaluate the actual impact (Both financial and reputational) on both the customers and service providers as a result of each of the above frauds.

From the study, we concluded that there are only 2 channels by which mobile network is initiated and propagated namely Short Message Service (SMS) and Voice but in most cases a combination of the two was utilized by the fraudsters. This situation might change with time as new channels emerge including email, mobile applications, and social media. With this regard case study should be done in the future to evaluate the impact of these new emerging channels.

The study also revealed that service providers are still using manual processes the detect fraud due to the dynamic nature of mobile fraud in Kenya. This exposes a huge gap in the detection process and there is a need to address this by developing systems and processes that will automatically detect these everchanging fraud patterns with minimal human intervention. A potential strategy to address this gap would be deployment of machine learning driven tools that will automatically learn and adjust to new fraud tactics. In the automated fraud detection processes, concept drift was established to be the main challenge in this process whereby the automated models gradually and even in some cases drastically reduce detection accuracy resulting in the misclassification of fraud cases. Due to this issue, the service providers fall back to the manual process. In this regard, a research gap exists in which a process that detects and corrects concept drift needs to be developed in the automated fraud detection processes. The cause of the concept drift was not very clear in this study on whether it was due to data change or it is a real drift and therefore the study would propose a qualitative study to be carried on to scientifically address this question. A true experiment approach can be used to identify the magnitude, causes, and points of drift on currently used automated tools. From the results, more advanced machine learning and deep learning tools can be developed to address this issue.

REFERENCES

[1] Rupa et al., 2015, Cellular Network Fraud & Security, Jamming Attack and Defenses Available at: https://pdf.sciencedirectassets.com/280203/1- s2.0- S1877050916X00026/1- s2.0- S1877050916000405/main.pdf?X-Amz-Security

[2] Ogwueleka, 2009 fraud detection in mobile communications networks using user profiling and classification techniques.

Article DOI: https://doi.org/10.37284/eajit.7.1.2212

Available at: https://core.ac.uk/download/pdf/37370566.pdf

[3] Yang et al. 2018, Mining Fraudsters and Fraudulent Strategies in Large-Scale Mobile Social Networks, Available at: https://ieeexplore.ieee.org/document/8744319

[4] Philip et al., 2015, On arbitration, arbitrage and arbitrariness in financial markets and their governance: unpacking LIBOR and the LIBOR scandal. Available at: https://www.researchgate.net/profile/Philip-Ashton- 2/publication/275556489_On_Arbitration_Arbitrage_and_Arbitrariness_in_Financial_Markets_and_Their_Governance_Unpacking_LIBOR_and_the_LIBOR_Scandal/links/5b10028faca2723d99775354/On-Arbitration-Arbitrage-and-Arbitrariness-in-Financial-Markets-and-Their-Governance-Unpacking-LIBOR-and-the-LIBOR-Scandal.pdf

[5] Snehal et al., 2019, Awareness of Sim Swap Attack.Available at: https://d1wqtxts1xzle7.cloudfront.net/59921743/215_Awareness_of_Sim_Swap_Attack20190703-77135-1etachf-libre.pdf?1562159287=&response-content-disposition=inline%3B+filename%3DAwareness_of_Sim_Swap_Attack.pdf&Expires=1718043928&Signature=MK9zvJb6Gps287s3jEyjpkvO9~9bEfb~dwP4l3Co2O9oqWO96DrTn7wzCH29Ua3Bm~1tOmFAxlD9IdYAgkXsfaXIgMW4okfjaR1dxmelM7qAVaWuU8VjCxgp2dOGUmc5K43DmebUySV~6s- 29e6NQOmI5deRql02yvQzRlMnanNZ-x5p7KR7ldVxQ0cidc6XhUCGCxtzVO8x~aie3Wgt0a2QCLyqi~4oCG1c8Tr7mlRFRb2mo0bB1lGWqXxTM0qjuJschVcxs-gzD2qydq-6jb1cuCwqux6~LSABs9LtazrW1UkQ3EuPbq1eXy7kw7xonn2Q1Rd4zkGcUx-bllV6Gg__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA

[6] Roger, 2023, SIM Swapping Attacks for Digital Identity Theft: A threat to financial services and beyond. Available at: https://www.researchgate.net/profile/Roger-Hallman/publication/376612643_SIM_Swapping_Attacks_for_Digital_Identity_Theft_A_threat_to_financial_services_and_beyond/links/658091b20bb2c7472bf3dd84/SIM-Swapping-Attacks-for-Digital-Identity-Theft-A-threat-to-financial-services-and-beyond.pdf

[7] Biju, 2022, SMS Fraud Detection Using Machine Learning. Available at: https://www.researchgate.net/profile/Soumya- Prusty/publication/360371905_SMS_Fraud_Detection_Using_Machine_Learning/links/628781c5cd5c1b0b34e95817/SMS-Fraud-Detection-Using-Machine-Learning.pdf

[8] David, 1996, Focus Groups.

Available at: https://www.researchgate.net/profile/David- Morgan- 43/publication/305389505_Focus_Groups/links/5bcaa150299bf17a1c61a4fe/Focus-Groups.pdf

[9] Carey, 1994, Capturing the Group Effect in Focus Groups: A Special Concern in Analysis. Available at: https://journals.sagepub.com/doi/abs/10.1177/104973239400400108

[10] ZhiYuan, 2020, Modeling Users' Behavior Sequences with Hierarchical Explainable Network for Cross-domain Fraud Detection. Available at: https://arxiv.org/pdf/2201.01004

[11] Tarmazakov et al., 2018 Modern approaches to prevent fraud in mobile communications networks. Available at: https://ieeexplore.ieee.org/abstract/document/8317111

[12] J Gama et al., 2013, On evaluating stream learning algorithms. Available at: https://link.springer.com/article/10.1007/s10994-012-5320-9

[13] Muriuki, 2017, Curbing Mobile Phone Terrorism and Financial Fraud: A Kenyan Perspective. Available at: https://www.researchgate.net/publication/317043444_Curbing_Mobile_Phone_Terrorism_and_Financial_Fraud_A_Kenyan_Perspective

Article DOI: https://doi.org/10.37284/eajit.7.1.2212

[14] Kala, 2021, Assessment of SIMBox Fraud: An Approach to National Security Threat. Available at: https://www.researchgate.net/profile/Kala- Baskar/publication/356914651_Assessment_of_SIMBox_Fraud_An_Approach_to_National_Security_Threat/links/61b71797a6251b553ab51ccc/Assessment-of-SIMBox-Fraud-An-Approach-to-National-Security-Threat.pdf

[15] Nassir, 2020, Study to use NEO4J to analysis and detection SIM-BOX fraud. Available at: https://scholar.google.com/scholar?hl=en&as_sdt=0%2C5&q=Study+to+use+NEO4J+to+analysis+and+detection+SIM-BOX+fraud&btnG=

[16] Mais et al, 2018, Detection of Wangiri Telecommunication Fraud Using Ensemble Learning. Available at: https://www.researchgate.net/profile/George- Sammour/publication/333232206_Detection_of_Wangiri_Telecommunication_Fraud_Using_Ensemble_Learning/links/5d07d7f5a6fdcc35c155c208/Detection-of-Wangiri-Telecommunication-Fraud-Using-Ensemble-Learning.pdf

[17] Jessica,2018, Detect & Protect Against Wangiri Callback Fraud.

Available at: https://www.enghousenetworks.com/enghouse- resources/blog/infographics/detect-protect-against-wangiri-callback-fraud/

[18] Krueger, 1997, Developing Questions for Focus Groups. Available at: https://books.google.com.qa/books?hl=en&lr=&id=odtyAwAAQBAJ&oi=fnd&pg=PP1&dq=Krueger+1997&ots=gjBWeEvMPc&sig=EkX2FXV3nNefwiYrX1vO9aNparo&redir_esc=y#v=onepage&q=Krueger%201997&f=false

[19] Geoffrey et al., 2016, Characterizing Concept Drift. Available at: https://arxiv.org/pdf/1511.03816

[20] Tsymbal, 2004, The problem of concept drift: definitions and related work.

Available at: https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=30eac73e9b482bc28b5b68cd585557de48d0618f

[21] Sumaya et al., 2021, An Enhanced Secure Deep Learning Algorithm for Fraud Detection in Wireless Communication Available at: https://onlinelibrary.wiley.com/doi/10.1155/2021/6079582

[22] Communication Authority of Kenya (CAK) report, 2019 Available at: https://www.ca.go.ke/sites/default/files/2023- 06/Customer_Satisfaction_Survey_Report_for_CA_June-2019.pdf

[23] Communication Authority of Kenya (CAK), 2023 Available at: https://www.ca.go.ke/kenyan-mobile-sector-records-growth-revenue-and-investments

[24] Braun et al., 2006, Using thematic analysis in psychology Available at: https://uwe-repository.worktribe.com/index.php/preview/1043068/thematic_analysis_revised_-_final.pdf

[25] Aisha et al.,2016, Fraud detection system: A survey Available at: https://www.sciencedirect.com/science/article/abs/pii/S1084804516300571

[26] Silverman, 2005, Improving the State of the Art of Qualitative Research Available at: https://www.qualitative- research.net/index.php/fqs/article/view/6/14

