EVALUATING THE ROLE OF TELECOMMUNICATION COMPANIES IN MITIGATING THE IMPACT OF SIM SWAP FRAUD

ANTHONY OGUNNA
2413689

An Assignment Submitted in the partial fulfilment for
the award of Master of Science degree in Data Analytics and Technologies

December 2024

The University of Bolton
Deane Road, Bolton, BL3 5AB
http://www.bolton.ac.uk

TABLE OF CONTENTS

ABSTRACT

SIM swap fraud has become a global threat to mobile phone users, as this is having adverse negative effect on the lives of victims financially, psychologically and otherwise. This research work explores the responsibility of telecommunication companies in mitigating the effect of SIM swap fraud through systematic prevention and intervention approaches and the efficacy of these measures. Employing a mixture of qualitative and quantitative methods, including survey of subscribers, with focus on the affected ones and interview of telecommunication industry professionals, this research evaluate the professional standard practices engaged by telecommunication companies to detect and prevent SIM swap fraud. The study also explores subscribers' alertness to sim swap fraud and awareness network providers have created in enlightening their subscribers on safeguarding their mobile accounts. Findings show that some network providers still have lapse in the SIM registration process of users, giving room for SIM hijacking and other SIM related scams. Although some telecommunication operators have incorporated advanced verification system and fraud detection structure into their network, there is still loophole in subscribers' engagement and prompt response to related issues. The study concludes by recommending advanced biometric registration process before the activation of a SIM for strict and effective data storage and protection, alongside collaborative synergy in data management and processing among network providers, financial institutions and regulatory bodies with more security framework to mitigate SIM swap fraud.

CHAPTER 1: INTRODUCTION AND RESEARCH APPROACHES

1.1 BACKGROUND STUDY

SIM swap fraud, also known as SIM card swapping or SIM hijacking is a form of identity theft where a fraudster gains control of an individual phone number by convincing the mobile network provider to transfer the phone number to a new SIM in the fraudster possession (Hallman,2023). This gives the fraudster access to the calls, messages, one time password (otp) and two-factor authentication sent to the victim's number, bank accounts and social media accounts, among others. The rapid growth of digital banking and online transactions has increased the risk and damages related with SIM swap fraud.

Fraudsters take advantage of the verification loopholes in the mobile network authentication framework, making it very crucial for network providers to explore all possible security means to prevent and mitigate this identity theft.

Some Mobile Network Operators still allow SIM swap process via phone call engagement, making it easy for fraudsters to impersonate their victims after gathering enough information about them as the network customer service provider on the other end of the phone conversation cannot see the caller to verify facial recognition. In some cases, there are no proper biometric information of the users as SIM are activated without biometric capturing and registration, making it easy for fraudsters to impersonate and swap victims SIM.

1.2 AIM OF STUDY

The aims of study are;

1) Identify the gaps and barriers in combating SIM swap fraud by telecommunication companies and provide recommendation to enhance SIM security.
2) Explore current practice in telecommunication companies with respect to SIM registration and security.
3) Examine Legal and regulatory structure.

1.3 RESEARCH QUESTIONS

In this study, we will be looking at the following research questions to enable us understand the importance of the subject matter and how to cover the gaps and find a lasting solution to the challenges associated with sim swap fraud. The following questions help us to dive into the security issues surrounding SIM security in telecommunication companies and possible ways to mitigate the effects. Below are some of the research questions;

1) What are the challenges and gaps in the mitigation of SIM swapping fraud?
2) What are the current practice and security measures in place by Telecommunication companies to combating SIM swap fraud?
3) What are the legal and regulatory frameworks that supports or hinder Telecommunication companies in combating SIM swap fraud?
4) What improvements can Telecommunication companies make to better mitigate SIM swap fraud?

1.4 RESEARCH OBJECTIVES

The research objectives which are specific and measurable action steps required to actualize the aims of the research work are as follows;

1) To identify the challenges faced by Telecommunication companies and gaps in preventing and mitigating SIM swap fraud.
2) To evaluate the efficacy of the current security measures and preventive efforts by Telecommunication companies in mitigating SIM swap fraud.
3) To examine the effectiveness of laid down Legal and regulatory frameworks in aiding Telecommunication companies in combating SIM swap fraud.
4)To provide feasible recommendation for Telecommunication companies to enhance their security framework in mitigating SIM swap fraud.

1.5 RESEARCH PROBLEM

The prevailing rise in SIM swap fraud has become a global security concern as its impact is imposing negative effects on its victims financially, psychologically and otherwise. It is a widespread issue with financial, emotional and social

consequence for its victims. The Telecommunication companies, being saddled with the responsibility of managing subscribers phone numbers are often the first level of defence against SIM swap fraud. However, despite the advanced technologies and identity authentication procedures, the occurrence of SIM swap fraud is still at a high level, making subscribers exposed to identity theft and other fraudulent acts, especially SIM swapping (Kim, Suh and Kwon, 2022). The shortcoming of Telecommunication companies in providing a formidable technological security for subscriber's sims against identity theft continue to be a critical challenge.

1.6 SIGNIFICANCE OF THE STUDY

The above study is of great significance in understanding the concept of SIM swap fraud, addressing its wider implications and recommending effective measures in mitigating its effects.

Below are some points that spotlight the significance of this research work:

1) Improvement on the security of subscriber's account.
2) Solutions for SIM swap fraud prevention.
3) Regulatory compliance and customers protection.

1.7 RESEARCH APPROACHES

1.7.1 Identification of three (3) research approaches.

The three (3) research approaches that could be apply to the above research topic are;

1) Realist
2) Pragmatism
3) Positivist

Realist: This paradigm refers to the existence of one single reality which can be studied, understood and experienced as a truth, and is independent of human perception. This paradigm is objective with measurable information that reflects real world events. Realism gives a philosophical viewpoint that is fitting with both qualitative and quantitative methodologies.

Pragmatist: This paradigm is a practical approach to research, focusing on problem solving and outcomes. It is less concerned with the discourse between objectivity and subjectivity and prioritize the practical outcome of research. The methodology used under pragmatism is mixed method, consisting of qualitative and quantitative methodologies.

Positivist: Positivism is a philosophical view that is established on the belief that reality exists independently of human perception, and is empirical and can be objectively measured. Quantitative methodology is most appropriate for this paradigm as it deals with empirical observations that are measurable.

1.7.2 Evaluation of research approaches.

1. Realist approach.

This approach relates to existence of one reality which is objective and independent of human perception. It lays emphasize on the importance of understanding the reality in its details. In the context of this research, realism would focus on the structural and social factors relating to SIM swap fraud, such as the technological loopholes, regulatory gaps and the socio-financial frameworks in which fraud occurs.

Strength

a) **In-depth evaluation:** Realist approach would allow for an in-depth exploration of the wider system that enables SIM swap fraud, evaluating the technological framework, regulations and professional practices in the Telecommunication industry.

b) Detailed analysis of interconnection: This would enable the research to focus on the interrelated components of SIM swap fraud mitigation such as weak technological security frameworks, subscribers' awareness and other possible vulnerability in the authentication protocols.

Weaknesses

a) **Difficulty in measurement:** Realism can sometimes be challenging especially when it focuses on detailed, often intangible components that may be difficult to measure empirically like practices, policies and regulations.

b) **Limited application**: Realism approach often focus on specific scenarios, so findings may not be applicable to other regions or Telecom market with different policies, regulations or technological environment.

Suitability

Realist approach is suitable for evaluating wider structural context in which SIM swap fraud occurs, such as industrial practices, role of regulations and relationship between stakeholders (Telecommunication companies, regulatory bodies, subscribers, etc)

2. Pragmatist approach

This approach focuses on the practical ways to resolving problems. In the context of SIM swap fraud, a pragmatist approach would focus on identifying the practical measures that telecommunication companies can employ to reduce fraud irrespective of theories or perceptions.

Strength

a) **Action oriented:** One of the remarkable strengths of this approach is its result driven quality. Pragmatist focuses on practical outcomes in alignment with actionable recommendation. In the context of SIM swap fraud, this approach would focus on most effective measures (e.g. stronger identity verification framework, enhancement of industry's practices, etc) in mitigating SIM swap fraud.

b) **Flexibility:** Pragmatism accommodates the use of multiple methods (quantitative, qualitative or mixed methods) in evaluating different aspects of the problem, giving room for flexible research design.

c) **Focus on involved parties:** This approach would focus on finding solutions to real life problems of the parties involved such as the Telecommunication companies, subscribers and regulators, giving room to a broader application of its findings.

Weaknesses

a) **Transient Focus**: Due to its target on actionable solutions, it may overlook long term strategic measures, giving for negligence of potential structural change in the future that may affect SIM swap fraud.

b) Insufficient theoretical depth: Inasmuch as pragmatism approach produces more resourceful findings, it may lack sufficient theoretical insight of other approaches such as realism and positivism, possibly leaving other causes of SIM swap fraud under-explored.

Suitability

This approach is highly suitable for research focused on evaluating the measures for mitigating SIM swap fraud as it allows for a practical exploration of real-life problems relating to the subject matter and providing recommendation which will help the Telecommunication companies improve their strategies in combating SIM swap fraud.

3. Positivist approach

This approach focuses on objective knowledge with empirical evidence, using scientific methods to evaluate issues. In the context of SIM swap fraud, this approach would focus on measurable data such as the frequency of SIM swap fraud, the efficacy of current technological preventive measures and measurement of other empirical metrics.

Strength.

a) Objective and empirical framework: One of the remarkable qualities of this approach is its high structured data driven procedure in evaluating measurable issues thereby helping researchers draw clear conclusion from SIM swap fraud data with the aid of statistical analysis, experiment and survey.

b) Measurable results: The focus on measurable data can help provide more clarified information on outcomes after exploring possible preventive measures.

Weaknesses.

a) Over simplification: By addressing mainly quantifiable observations, positivism may ignore other social and industrial factors that contribute to SIM swap fraud, thereby giving room for scanty understanding of the subject matter.

b) Reductionist: Due to its empirical qualities, positivism tend to reduce detailed events into numerical data which may not fully capture other categorical information of SIM swap fraud.

Suitability.

This approach is mainly suitable in measuring quantifiable information relating to SIM swap fraud such as numerical feedback after implementing a fraud mitigation measure, and this may be less suitable in evaluating a wider context of the issue such as the structural deficiencies, regulations, etc.

1.7.3 Justification of Pragmatist approach as the most appropriate.

The pragmatist paradigm is the most suitable for this research as this gives a better approach for a well-rounded study, combining the quantitative and qualitative methods for a holistic exploration of the subject matter. This approach will evaluate the most effective technological measures in mitigating SIM swap fraud, scrutinize the industrial practices, examine polices and regulations, and provide recommendation to help Telecommunication companies combat SIM swap fraud, not neglecting subscribers' protection.

1.7.4 ETHICAL CONSIDERATION OF RESEARCH APPROACH

The ethical consideration of the pragmatist approach focuses on the effect of research decision on the stakeholders involved (telecommunication companies, the subscribers, the regulatory bodies and ethical guidelines). Under the use of the pragmatist approach, the following ethical issues are taken into consideration:

1) **Prioritizing positive outcome:** The pragmatic approach should focus primarily on providing actionable solution to the real-life problems associated with SIM swap fraud. Researchers should ensure that their findings are geared towards helping the stakeholders by recommending more effective solutions in enhancing identity authentication security to reduce fraud.

2) Confidentiality and data privacy: One of the major ethical considerations in evaluating the role of telecommunication companies is the protection of sensitive data. If the research involves data of SIM swap victims, it is very important to anonymize and maintain confidentiality with compliance to data protection policies of GDPR and other local privacy regulations.

3) Informed consent and transparency: If victims of SIM swap fraud or employees of telecommunication companies are involved in the research, it is crucial to get informed consent from all participants and clearly explain the purpose for the research and how their data will be used.

4) Social justice and equity: Researchers should ensure that the outcome of the research does not aggravate the issue of social inequalities and the recommendation does not affect any group of people e.g., the elderly, those in rural areas, low-income earners, etc.

5) Responsibility to the public: The primary goal for evaluating the role of telecommunication companies in mitigating SIM swap fraud is for interest of the public. Researcher should ensure that their findings are accessible to the public in simple and understandable terms.

CHAPTER 2: LITERATURE REVIEW

2.1 SUMMARY OF LITERATURE REVIEW

The issue of SIM swapping is a serious concern across the globe. The perpetrators of this fraudulent act capitalize on the security loopholes in SIM protection to hijack their victims SIM card by convincing the network provider to modify the SIM card the fraudster is holding with the one linked with a victim's account (Lee et al., 2020). This concern has led to many research works with the objective of mitigating this identity theft. Different researchers came up with different recommendations which include building a more robust security system in the telecommunication industry, creating more awareness and enlightening subscribers on fraudsters schemes and necessary precautions to be taken among others (Awale and Gupta, 2019). In the course of this research work, literature was reviewed for better background understanding of the subject matter, among which ten (10) pieces of literature were critically analysed with respect to their methodology, findings, conclusions and gaps. Below is a concise overview of the ten literatures analysed.

2.2 COMPARISON OF LITERATURE

Table 2.1

NAME OF AUTHOR / BRIEF INTRODUCTION	METHODOLOGY	FINDINGS	CONCLUSION
Bhavana, Miriam and Robin (2024). This research focus its SIM swap fraud mitigation measures mainly on subscribers, outlining key preventive measures and other safety precautions.	Qualitative analysis, (case study and literature review).	Easy access to personal data contributes immensely to SIM swap fraud.	Enabling two factor authentication. Changing PIN regularly and not sharing one time password are good preventive measures for SIM swap fraud

Lee et al., (2020). This study sought to reverse-engineer the policies for SIM swaps at five U.S. network providers—AT&T, T-Mobile, Tracfone, US Mobile, and Verizon Wireless with the aim to evaluate their authentication procedures, compare the SIM swap process between their prepaid and postpaid accounts and recommend more secured measures to combat SIM swap fraud.	The methodology combines quantitative and qualitative analysis in addition to comparative analysis for prepaid and postpaid accounts.	The researchers observed that postpaid accounts are more secured than prepaid accounts. And automatically enrolling subscribers in SMS based multi factor authentication weakens the security procedure.	Recommend authentication via app login or otp via voice call.
Kim, Suh and Kwon (2022). The SIM swap procedures and prevalence of five (5) countries are taken into consideration in this study.	Qualitative analysis (case study)	Case study of global trend in SIM swapping in UK, US, Nigeria, Canada and Korea need more government intervention in enforcing strict authentication policies.	Authentication procedure need to be more app based such as biometric and PIN in order to address the interception of otp by fraudsters
Awale and Gupta (2019). This study gives awareness about SIM swap attack, its prevalence and how the attack occurs in sim on mobile phone. And went further to provide protective insights against the attack.	Qualitative analysis (descriptive research and case study)	The findings are limited to how fraudsters swap victim's sims.	The conclusion is limited to the prevalence of SIM swap attack.

Faircloth et al., (2022). This research x-ray the 2021 T Mobile breach carried out by John Binns, a hacker, resulting in the theft of fifty four million customers' data which eventually opened door to SIM swap fraud.	Qualitative analysis (exploratory research and case study)	Theft of customers data opens door to SIM swap fraud	The researchers recommended defensive measures such as identity theft monitoring services for additional protection, stored data encryption and password security for both the subscribers and telecommunication companies.
Rosa, (2024). The research approaches the SIM swap process as a "security ceremony," which involves a stratified analysis of technical procedures and human interactions	Mixed method (Qualitative and quantitative analysis)	The introduction of Pirandellian masks gives a resourceful model for understanding the interaction of human entities in SIM swap security procedure	The study highlights the importance of integrating both technical and human dimensions (Human - technology interaction) in boosting security against SIM swap fraud.
Marakalala, (2023). This study focuses on the effectiveness of biometric-based solution to mitigate Mobile Fraud at the South African Risk Information Centre.	Qualitative analysis (Literature review)	The researcher observed that the techniques used by criminals, include mobile device hijacking and the scheming of sensitive financial data to launder money.	The researcher concludes that biometric verification is crucial to mitigate mobile fraud, as it provides more advanced security that conventional verification protocol cannot provide.
Ali et al., (2019). Internet, mobile and traditional telecommunication are the key attributes in this study and are viewed from the standpoint of	Qualitative analysis (Comparative research)	The researcher observed that fraud is prevalent in browser based and mobile internet services.	The researchers recommend stronger security measures such as advanced fraud detection technologies and stronger regulatory structures to combat mobile fraud.

identity theft. In addition, the study also provides recommendations for security from mobile fraud and attacks.			
Akinbowale, Mashigo and Zerihun, (2024) This study evaluates the challenge of financial fraud with focus on cyber fraud	Mixed method (empirical analysis, systematic literature review and case studies)	The research identifies digital technologies for business transactions as one of the key activities triggering cyber fraud	The research concludes that cyber fraud mitigation requires a multi-dimensional approach that integrate high level technologies, theoretical models, and practical solutions.
Dey, (2019) This study focusses on understanding identity theft in online banking by analysing set of reported cases with respect to meta data of user accounts to identify recurring pattern for detection.	Mixed method (metadata)	The research points out that identity theft may appear unique but shared common trend across certain cases, making it possible to predict identity theft by identifying recurring patterns.	The research concludes that identity theft detection in online banking can be enhanced by evaluating account meta-data to identify behavioural patterns that are consistent across cases.

2.3 RESEARCH GAPS

Table 2.2

NAME OF AUTHOR	YEAR	RESEARCH GAPS
Bhavana, Miriam and Robin (2024)	2024	Preventive measures were limited to only the subscribers' taking precautions with no evaluation on the telecommunication companies security measures

Akinbowale, Mashigo and Zerihun,	2024	The research is limited to categorical analysis without in-depth evaluation of the security measures for fraud mitigation.
Rosa	2024	The research focused on modelling human behaviour which may not give sufficient solution as the issue of SIM swap is a global concern with billions of subscribers.
Marakalala	2023	The research is limited to money laundering via mobile fraud.
Kim, Suh and Kwon	2023	Left diversification of authentication factors to future research.
Faircloth et al.	2022	The flexible telecommunication practices that create loopholes for SIM swap fraud were not evaluated.
Lee et al.	2020	This research only advises telecommunication companies to come up with optional online authentication procedure without recommending a better security measure.
Awale and Gupta	2019	The research failed to give protective measures against SIM swap attack.
Ali et al.	2019	The research fails to explore the practices in the telecommunication industries for effective implementation of security measures.
Dey	2019	The use of recurring patterns to detect identity theft may not be effectively feasible as a limited number of cases may be taking into consideration during analysis.

2.4 BRIDGING EXISTING KNOWLEDGE GAPS

From the literature review, in-depth evaluation of the telecommunication practices with respect to how a new user is onboard is missing. A proper review of this part of the activation process is very crucial as it is the foundation of the SIM history of the user. To effectively secure a subscriber's SIM, the first registration before the SIM is activated is very key as it is the basis on which further authentication will be carried out. This research will examine this sensitive aspect of SIM activation with a holistic view of the biometric capturing process, recommending facial and fingerprints capturing alongside other registration procedures before a SIM will be activated. With this practice, it will

be difficult for a fraudster to impersonate the victim during SIM swapping as the fingerprints and facial recognition are unique to the subscriber. Phone call SIM swap process should be reviewed as fraudsters hide behind this loophole to claim the identity of the victim since the customer care representative cannot see the person on the other end of the call to verify the authenticity of the caller. In addition, this research will recommend creation of retail outlets by telecommunication companies in different strategic areas where subscribers can walk in for proper identification from the facial and fingerprints information captured when they first registered the SIM before any swap can be carried out on their SIM.

2.5 HOW LITERATURE REVIEW INFORMS THE RESEARCH.

Analysis of the literature informs the research design and methodology chosen in chapter one as this approach will address the need for better telecommunication industry practices, enhance fraud prevention measures, and the importance of strong legal and regulatory policies to support combat against swap fraud. The research will be designed to address gaps identified in the literature. By combining both quantitative data and qualitative insights, the research will provide a detailed evaluation of telecommunication companies' role in mitigating SIM swap fraud.

2.6 CONCLUSION

This study highlights the pervasive and damaging impact of SIM swap fraud on mobile phone users, demonstrating that the consequences extend beyond financial loss to include psychological and social repercussions. The research underscores the critical role of telecommunication companies in mitigating such fraud through both preventive and responsive measures. Findings indicate that, despite the adoption of advanced verification systems and fraud detection mechanisms by some operators, significant vulnerabilities remain in SIM registration processes and subscriber engagement. These gaps continue to expose users to potential SIM hijacking and related scams.

To address these challenges, the study recommends the implementation of a robust biometric registration system prior to SIM activation, ensuring more secure data storage and verification. Furthermore, it advocates for strengthened collaboration among network providers, financial institutions, and regulatory bodies to enhance data management, streamline response protocols, and establish a comprehensive security framework. By integrating these measures, telecommunication companies can more effectively safeguard subscribers, reduce the prevalence of SIM swap fraud, and reinforce public trust in mobile communication systems.

REFERENCES.

Lee, K., Kaiser, B., Mayer, J. and Narayanan, A., 2020. An empirical study of wireless carrier authentication for {SIM} swaps. In *Sixteenth symposium on usable privacy and security (soups 2020)* (pp. 61-79).

Kim, M., Suh, J. and Kwon, H., 2022, August. A Study of the Emerging Trends in SIM Swapping Crime and Effective Countermeasures. In *2022 IEEE/ACIS 7th International Conference on Big Data, Cloud Computing, and Data Science (BCD)* (pp. 240-245). IEEE.

Ekeh, G.E., Afolabi, Y.I., Uche-Nwachi, E.O., Ekeh, L.K. and Eze-Udu, E., 2022. Awareness of BVN, SIM swap and clone frauds: Methods and controls. *Science World Journal*, *17*(2), pp.200-206.

Egal, L.A., Chief, B., Bureau, E. and Egal, D.B.C., 2024. including conducting assessments for potential network-level vulnerabilities and investigating instances of SIM swap/port-out fraud.

Varghese, E. and Pramila, R.M., 2022. Protection Against SIM Swap Attacks on OTP System. In *Data Science and Security: Proceedings of IDSCS 2022* (pp. 219-228). Singapore: Springer Nature Singapore.

Murugalakshmi, S. and Robin, C.R., 2023. Advancements in mobile security: A comprehensive study of SIM swapping and cloning-trends, challenges and innovative solutions. *I-Manager's Journal on Mobile Applications & Technologies*, *10*(1).

Alghawi, N., 2019. *A Study on SIM Box or Interconnect Bypass fraud* (Master's thesis, The British University in Dubai).

Valentine, J.P., 2021. *Sim Card Fraud* (Master's thesis, Utica College).Awale, S.M. and Gupta, D.P., 2019. Awareness of sim swap attack. *International Journal of Trend in Scientific Research and Development*, *3*(4), pp.995-997.

Salaudeen, L.G., Yauri, A.R., Muhammad, G., Umar, H. and Aliyu, S., 2022. A Plethoric Literature Survey on SIMBox Fraud Detection in Telecommunication Industry.

Faircloth, C., Hartzell, G., Callahan, N. and Bhunia, S., 2022, June. A study on brute force attack on T-mobile leading to SIM-hijacking and identity-theft. In *2022 IEEE World AI IoT Congress (AIIoT)* (pp. 501-507). IEEE.

Akinbowale, O.E., Mashigo, M.P. and Zerihun, P., 2024. Understanding and mitigating cyberfraud in Africa.

Marakalala, M.C., 2023. Forensic Intelligence: The Effectiveness of the Biometric-based Solution to Combat Mobile Fraud. *OIDA International Journal of Sustainable Development*, *16*(05), pp.19-30.

Rosa, L.G., 2024. Modeling the SIM Swap Ceremony: Integrating Human Behavior and Formal Analysis.

Bhavana, S.U., Doreen Hephzibah Miriam, D. & Rene Robin, C.R. 2024, "Understanding the Implications of SIM Card Swap Fraud in India: A Comprehensive Study", IEEE, , pp. 1.

Ali, M.A., Azad, M.A., Centeno, M.P., Hao, F. and van Moorsel, A., 2019. Consumer-facing technology fraud: Economics, attack methods and potential solutions. *Future Generation Computer Systems*, *100*, pp.408-427.

Dey, K.A., 2019. *Mitigation of Identity Theft in Online Banking* (Master's thesis, The University of Bergen).

Hallman, R.A., 2023. SIM Swapping Attacks for Digital Identity Theft: A threat to financial services and beyond.