Exploring Methods Cybersecurity Managers Need to Implement to Minimize Cyber-Frauds in Mobile Money Services in Ghana

Bright Siaw Afriyie
bsiawa@sabsoftech.org
Sab-Softech Inc
1129 Beechwood Ln, Cedar Hill, TX 75104

Samuel Sambasivam
Samuel.Sambasivam@Woodbury.edu
Computer Science Data Analytics
Woodbury University
Burbank, CA 91504

Abstract

Nearly half the adult population in developing nations lacks a formal bank account and other financial services. Ghana is no exception, having a massive community of unbanked adults and among those countries positioned at the bottom of the spectrum of financial inclusion. The unbanked populations inconveniently indulged in physical cash-carry in every business transaction. The advent of mobile financial services (MFS) claims an alternative mode to financial inclusion. MFS, fundamentally implemented using SMS and USSD code, essentially encompasses mobile wallets, cash out, and over-the-counter transactions overgrowing globally, has a vast potential to minimize impediments to financial inclusion. However, mobile financial services' sustainability is threatened by cybercriminals or fraudsters while reaching increasingly a higher global penetration yearly. This qualitative exploratory study aimed to be explored security methods cybersecurity managers needs to implement to minimize cyber fraud of mobile financial services in Ghana. The research purports to identify viable methods leaders of MFS operators need to implement to reduce fraudsters' threats. The exploratory design was used as the lens to explore this phenomenon in-depth. A sample size of seven and 12 semi-structured interview questions were used as a data collection instrument. Lack of proper security methods and internal control processes were identified as the major causes of cyber fraud in MFS. Seven databases (Web of Science, ProQuest, ABI, EBSCO, IEEE, Sage, Google Scholar, Pub/Med, and Scopus) were searched using standard and adapted search syntax. The study also provided four recommendations on the ecosystem and the processes needed to utilize mobile technology's full potential.

Keywords: Mobile Network and Financial Service, Mobile Money Fraud, Mobile Security Architecture, Unbanked Financial Inclusion, Cryptography.

1. INTRODUCTION

The global economy is increasingly expanding mobile financial services. Developing countries represent the global leader in mobile financial services (Akomea-Frimpong et al., 2019). Mobile money popularly referred to as "MoMo" or "mobile wallet," is a financial technology (FinTech) offering unbanked people the possibility to use a mobile phone to transfer, receive, deposit, and spend money rather than carrying physical cash. Depending on the country, mobile money is named based on specific services such as mPesa, EcoCash, GCash, Tigo Pesa, etc. According to Nicco-Annan (2020), there were over 270 mobile money services worldwide; however, they were

most present in Africa, Asia, and Latin America. In developing nations, where the unbanked population was significantly high, MoMo emerged as a suitable alternative to cash, formal banking, and financial transactions since it was considered easy to use, secure and accessible anywhere there was a mobile phone signal (Akomea-Frimpong et al., 2019; Nicco-Annan, 2020). The mobile financial service covers a full spectrum of financial services, from payment transactions and checking to savings accounts, loans, insurance, and investments (Chironga et al., 2017). The proliferation is expected to extend to media and entertainment, web services, retail, and healthcare by 2024 (Ingle, 2019; Normans Media Ltd, 2017).

The MFS has predominantly gained roots in developing nations, particularly in Africa. In a sub-Sahara country like Ghana, the number of cellular or mobile registered voice subscribers in March 2020 stood at 41,959,298 (National Communications Authority, 2020). Out of 32.7 million registered mobile money accounts, 14.7 million remain active, with 235,000 active operator agents (Bank of Ghana, 2020) for all four major mobile service providers operating in the country. According to Boateng (2018), about 83.1% of Ghanaians have mobile money accounts, while Naomi Kwetey et al. (n.d.) asserted that the unbanked population was estimated at 70% of the entire population. Mobile Telecommunications Network (MTN), a leading company and the first to introduce MFS in 2009, now has 23,945,672 registered subscribers, representing 57.07 percent of registered subscribers in Ghana. Vodafone followed in 2011 with 8,787,464 subscribers, representing 20.94 percent of registered subscribers in Ghana, Airtel-Tigo with 8,498,008 subscribers representing 20.25 percent, and Glo with 728,154 subscribers representing 1.74 percent of registered subscribers (National Communications Authority, 2020).

With about 13.05 million active subscribers, the mobile money industry realized a cash transaction value estimated at GHC223.2bn (US$ 43bn) in 2018. In 2019, this value jumped to GHC265.42bn, with 25.78 million active registered subscribers being 26% over the previous year (Botchey et al., 2020). The drive continues as mobile money's market size expects to grow from USD 21.15 billion in 2016 to USD 112.29 billion by 2021, and MoMo payments are expected to compound an annual growth rate (CAGR) of 22% by 2024 (PR Newswire, 2019). IndustryARC (2019) projected a CAGR of over 24.9% growth in the forecast period 2021 to 2026.

The Ghana Interbank Payment and Settlement Systems (GhIPSS) reported that mobile money interoperability (MMI) increased by 358% during the first quarter of 2020 (Nicco-Annan, 2020). This upsurge is causing an exponential expansion of the cyber surface, creating numerous opportunities for cyber fraudsters (Weber & Studer, 2016). The cyber fraudsters continued to exploit vulnerabilities associated with deficiencies in proper security in the mobile money market; this has immensely attracted the need to identify and develop appropriate countermeasures against cyber fraud threats (Singh & Kumar, 2018). In Sub-Saharan Africa, including Ghana, 564 million mobile phone users suffered a cellular penetration rate of 65% in 2013. The figure was expected to reach 947 million in 2020, a penetration rate of 91%. Akomea-Frimpong et al. (2019) posited that mobile money services transactions lacked internal controls, efficient methods, and tools to curb the threats. Kanobe et al. (2017) affirmed the existence of literature gaps regarding MFS's information security management in developing economies, particularly reviews on the mobile money industry insider employees' roles in securely protecting the MFS business. According to Kyeremeh (2018), Delta3 International reported that in 2016 Ghana lost 50.0 million USD to cyber-related attacks. In Africa, the figure was approximately 2.0 billion USD –(GhanaWeb).

The study used the exploratory qualitative method to identify effective security methods cybersecurity managers need to implement to minimize digital fraud in mobile financial services in Ghana (Guma et al., 2020). In essence, it intended to provide recommendations to increase the safety of vulnerable populations engaging in electronic financial transfers in developing countries at risk. Akomea-Frimpong et al. (2019) articulated that MFS fraud is a salient economic problem; however, little has been captured in the research literature. The study further sought to fill this literature gap. The research used the game theory to explain the phenomenon's underlying concepts. The theory binds the concept based on the Diffusion of innovations and the model of planned behavior (Weigel et al., 2014) to relate to Cybersecurity and information systems assurance research.

2. HISTORICAL FACTS OF THE UNBANKED

The historically unbanked population had suffered in a way to deliver profitable business, as they

had to carry physical cash. They banked their funds in their homes and carried cash for all business remittances and acceptance. Global remittances have been slow, less effective, inefficient, and very expensive for consumers, yet remittances are crucial for so many businesses worldwide (Bettman & Harris, 2014). Small and medium-sized businesses typically unbanked have been challenged with armed robbery and burglary in many instances while transporting physical discharge of their routine business activities. MFS represents a digital disruption that has started to move the industry forward through the opportunity of mobile devices to drive revolutionary change in the US$550bn remittance market, driving exponential change. With MFS, there is no more inherited infrastructure and expensive processes in doing business. Described as an innovative FinTech, MFS is reshaping the digital market structure, how investors and consumers receive and use the information and financial services, and how companies access and deploy capital. MFS processes ranging from new digital payment systems and digital or electronic currencies to online investment and finance platforms and data analytics are already impacting traditional financial markets and services (Brummer & Gorfine, 2014).

3. RESEARCH PROBLEM

The problem is the lack of efficient methods cybersecurity managers need to implement to minimize cyber fraud in mobile money services in Ghana (Akomea-Frimpong et al., 2019; Guma et al., 2020; Novelan et al., 2018; Singh & Kumar, 2018). The lack of proper protection methods or MFS not adequately protected creates opportunities for cyber fraudsters to hack mobile systems and steal customers' money. Bank of Ghana reported that Ghana lost over GHc 12.8 million (USD2.2million) in 2021 to mobile money-related fraud (Thebftonline.com, 2022). Security methods remain a salient problem in mobile money systems regarding using short message services (SMS) and unstructured supplementary service data (USSD) with inherent vulnerabilities (Novelan et al., 2018). Eavesdropping and intercepting money transfer data in transit posed significant security concerns for several mobile money ecosystems. No scheme or existing method could offer complete SMS and SS7 security (Khozooyi et al., 2009; Novelan et al., 2018). Lee and Narayanan (2021) found that out of 259 samples of recycled mobile phone numbers available to new subscribers in the United States at two significant carriers, 171 were tied to existing accounts, exposing security and privacy risks to potential hackers to exploit. No substantial research has been conducted to reduce these threats. The menace continued seriously affect mobile transactions' integrity (Maseno et al., 2017). Kisekka (2019) noted that according to MTN Uganda, some suspicious individuals obtained PINs from customers under pretenses and subsequently withdrew funds from customers' mobile money accounts.

The pertinence of the problems articulated led to the research question: *Q1*: What methods do cybersecurity managers need to implement to minimize cyber fraud in mobile money services in Ghana?

4. RESEARCH METHODOLOGY

This qualitative exploratory study aimed to explore security methods cybersecurity managers need to implement to minimize cyber fraud in Ghana's mobile financial services (MFS) (Akomea-Frimpong et al., 2019; Guma et al., 2020). Qualitative exploration was best suited as it attracted securing in-depth information-rich data (Bazen et al., 2021; Leedy & Ormrod, 2016). Adopting the Constructivist approach (McSweeney, 2018) focused on the target sample population of lived experience. Exploratory Design was used as a lens to capture the in-depth information stemming from 12 semi-structured interview questions from seven participants (Levitt, 2021). The exploratory Design satisfied the choice of interview participants in this qualitative study to produce additional meaning that made more sense.

5. CONCEPTUAL FRAMEWORK

The underlying conceptual framework for this study was based on the game theory. The game theorists strive to understand conflicts and cooperation in more complicated real-life situations to comprehend real competitive conditions (Smith, 1982). According to Osborne (2004), a game theory endeavors to help understand situations in which opposing decision-makers interact. Generally, a game is a competitive activity in which players compete based on rules. Myerson (2013) described game theory's language as a game referring to any social situation which involves two or more individuals called players. In-game approach, two fundamental assumptions rely on game theorists who constitute players made of (a) rational and (b) intelligence. The gamers also represent rational decision-makers if they make decisions in the consistent pursuance of their objectives. Building on judgment, the theory's fundamental results assume that each player aims to maximize

the expected value of the payoff measured on a specific utility scale. This decision, according to Amoroso and Magnier-Watanabe (2012), identified eleven key-related variables which have been blended into nine: (1) perceived ease of gaming and risk; (2) attitude toward game; (3) facilitating conditions; (4) perceived value and usefulness; (5) perceived security and privacy; (6) social influence; (7) trust; (8) behavioral intention to game; (9) the attractiveness of alternatives. The idea is that a rational decision-maker must make decisions based on maximizing the expected utility payoff (Von Neumann & Morgenstern, 1947) via favorable winning methods.

Based on Kolokoltsov and Malafeyev's (2020) affirmation, every human being strives to accomplish their essential goals at any stage while establishing permanent contact with others trying to achieve their purposes. People sometimes attempt to outsmart an opponent and occasionally establish alliances with cronies with similar interests. The theory was constructed under the premise of committing no mistakes. An atom of a single error or negligence of any player would certainly favor its opponent.

Similarly, bringing the concept down to a cybersecurity protection environment, flaws in any defensive mechanisms would favor the attacker who consistently searched for them. The framework illustrated that humans remain in a strict perpetual dichotomy in cyber warfare in which everyone strives to survive by winning over the other party. The game theory concept outlines three parties struggling in cyberspace: defenders or security experts, cybercriminals or intruders, and the target game zone comprising society, industries, government, and academia, which must be protected against cyberattacks.

6. POPULATION AND SAMPLE

The target population or universe comprised a set of people of interest that provided appropriate responses to the research question (Naseri, 2021; Sekaran & Bougie, 2010). The target population more suited for this study were people in mobile network operations with lived experience relating to the phenomenon under investigation (Creswell, 2014; Osborne & Grant-Smith, 2021)). The target demographics group was at least 18 years of age with a minimum of three years of work experience in cybersecurity or mobile network operations. The participatory population included professional cybersecurity managers and mobile network operator (MNO) managers in mobile phone corporations. Seven out of 10 purposeful samples recruited for this qualitative exploratory design were more suited for in-depth interviews. Getting a group targeting or sampling from a broader population range in various organizations provided diversity; primarily, selecting participants through the random sample addressed trustworthiness. Additionally, the purposeful sampling used for most qualitative research could address research bias and eliminate any unknown influences in the group targeting process (Editorial Board, 2016, p.47).

7. DATA ANALYSIS

To provide a meaningful understanding, an in-depth analysis of the data produced two categories, principal themes and popular topics, which summarized the critical points from the data collected. The principal themes represented the essential matters of the subject participants mainly elaborated on their insight. Popular topics covered less frequently mentioned findings but remained the main topics aligned with and strived to answer the central research question: what methods do cybersecurity managers need to implement to minimize cyber fraud in mobile financial services in Ghana? The six themes signified the main point of this study and interpreted a clear sense of the aggregated data collected as indicated in table 1. From the impartial assessment, five major themes and one popular topic emerged from the data. In total, six themes emerged from the participants' responses, which provided an understanding of the phenomenon. The themes isolated a central topic focusing on the methods for operational improvements.

Principal Themes and Popular Topics	50	100%
Participants Major Themes		
Security Improvement Methods	18	36%
Vulnerability Detecting	12	24%
Risk and Threat Assessment	7	14%
On-Boarding Process	5	10%
Phishing Scam Control	4	8%
Popular Topic		
Operations Improvement Process	4	8%

Table 1: Participants Data Principal Themes and Popular Topics

The themes were generated from Nvivo 12 Pro software with codes principally centered on cybersecurity methods and mobile security.

Principal Theme 1: Security Improvement Methods

The study unraveled that the mobile money ecosystem consisted of three principal actors ascertaining what Guo and Bouwman (2016) pointed out: the mobile users or holders of money accounts, the service provider or telecommunication companies, and the mobile money agents (Botchey et al., 2020). The methods used to detect mobile money fraud have been based on rules. The security improvement methods predominantly touched the operations of these three stakeholders in the MFS business. As the focus was on improving security in the mobile systems to be as resilient as possible, it would entail implementing at least baseline controls, including access controls, risk management, and personal security (Mtaho & Mselle, 2014). A baseline security process centered on the CIA triad configuration, embracing confidentiality, integrity, and availability (Shin et al., 2013) would require more stringent access authentication configurations such as two-factor authentication (2FA) and secure password mechanisms. The study has revealed that swapped SIM would work in any cellular phone registered in the same carrier or any unlocked phone from a different carrier. Still, unless the swapper obtains the PIN Code from the original SIM's registered owner, the attacker cannot access the victim's mobile account. A visible interaction aspect of the security objectives on IT business objectives was the frequent patches updates, which often slowed down system performance. Patches often installed late in schedules became less effective

The study findings revealed that almost all mobile telecoms in Ghana implement the GSM basic architecture blended in 2G, 3G, and 4G or LTE because of the evolution of technologies and compatibility of different brands of mobile handsets. It is worth pinpointing that none of the telecoms in the nation deploys a 5G network. While telecoms in Ghana embrace 2G and 3G technologies, advanced countries like the USA have AT&T telecom company discontinued deployment of 3G technology that could no longer support VoLTE (Voice over LTE) as of February 2022, according to Spectrum TV news channel. These telecom firms view the profitability only on the business side, embracing low-end devices without considering the security vulnerabilities such technologies embed. Mobile Networks using outdated technologies harbor vulnerabilities that attract many security threats like DDOS (Yin et al., 2018), brute force attacks, and system intrusions, with unsolicited SMS text messages and fake promotions ads. Security improvements could be implemented by making most of the 5G architecture features embedding SDN technology (Yao et al., 2019).

The mobile network runs Advanced Encryption Standard (AES) encryption algorithms with a key length greater than 128-bits. However, among several attack vectors against AES encryption, brute force appears as a known attack (Burr, 2003), and biclique cryptanalysis (Bogdanov et al., 2011) can lead to breaching the protection of mobile services. As Bogdanov et al. (2011) asserted and confirmed in a recent Sowmiya and Malarvizhi (2022) study about security for machine intelligence-based cryptosystems. Using an increasingly AES encryption key length of 256-bits would guarantee acceptable and trusted standards in the mobile systems would improve security. AES-256 appeared to offer one of the most difficult challenges in block cipher cryptanalysis for over a decade, requiring $2^{254.4}$ computational complexity to break it.

Principal Theme 2: Vulnerability Detecting

The methods for detecting mobile money fraud have been based on rules (Yadav & Sora, 2021). As revealed in this study, fraud detection must align with the top 10 OWASP and CVSSv3 vulnerabilities daily guides. The tools often used were penetration testing, threat modeling, intrusion detection and prevention systems (IDS)/(IPS), endpoint detection devices, and firewall filtering systems. The massive mobile money transactions (MMTs) also presented potential security challenges to telecom firms. Machine and deep learning methods have lately emerged as efficient financial tools to detect and prevent fraudulent activities (de Sá et al., 2018; Hajek & Henriques, 2017; Sadgali et al., 2019; Singh et al., 2012). The support vector machine (SVM), k-nearest neighbor (knn), and artificial neural network (ANN) are machine learning algorithms experts could deploy to predict possible fraud occurrences and prevention (Saxena et al., 2019).

Fraud detection thus plays a vital role in providing firm data assurance. Ponnusamy et al. (2020) enounced that social engineering's catastrophic effect has caused the industry to build adequate security infrastructure. The mobile network operations (MNO) employees must receive sufficient awareness training to combat social engineering attacks (Salahdine & Kaabouch, 2019). It was mind-boggling to discover that most MFS agent operators in Ghana did not receive formal security awareness training. Adopting Big Data Analytics (BDA) methods, as Gupta et al. (2018) noted, has the potential to

detect fraud. Detecting critical fraud data, BDA allows verifying fraud insights to react in real-time, investigate suspicious activities and analyze historical data based on fraud and financial crime patterns (Ranjan & Foropon, 2021). The study supported the highlights pronounced by Guma et al. (2020) regarding digital money mobile account security being prone to severe vulnerabilities affecting the safety of MoMo.

The USSD holds severe vulnerabilities. However, it functions as a real-time protocol for mobile communication technology used in GSM network architecture to deliver supplementary services for text exchange among mobile handset devices and application programs, avoiding access to the internet (Nyamtiga et al., 2013; Talom & Tengeh, 2019). The SS7 supports signaling to network elements without a direct trunk connection ((Lei et al., 2021; Paganini, 2016)). Discovery in this study was associated with participants' assertion that the SS7 protocol has a long-standing vulnerability that has never been fixed. In GSM architecture, weak encryption of broken stream cipher is optional, which occurs only with the traffic in the airway between the Mobile Station (MS) and the BTS or the cellular tower. The message contents spread in the air in plaintext at transmission time without any intrinsic security countermeasure (Chaeikar et al., 2021). Undeniably, this process presents a serious risk because the providers' operation staff could access and manipulate the SMS information on the SMSC. Therefore, SMS usage for mobile money transfers has enormous security concerns (Chaeikar et al., 2021), exposing threats such as eavesdropping, interception, and text modification.

Principal Theme 3: Risk and Threat Assessment

The study finding confirmed that although the MNOs engaged in an inhouse Risk Assessment Framework for detecting and mitigating vulnerabilities effectively, they leaned heavily toward using the NIST SP 800-30 and ISO27005 Risk Assessment framework as a central focus of their security program. The findings revealed that by applying the threat models described in NIST SP 800 53 standards, mobile network operating firms would be better prepared to detect and mitigate threats (NIST, 2020). Besides, threat identification was based on knowledge or skills, risk assessment, and utilization of threat modeling. The threat modeling appeared to pull tremendous knowledge from empirical research findings on attackers' activities all over the globe. The industry conducts risk assessments every quarter. One of the best practices in sourcing data from threat Intelligence would be to focus on potential threats, evaluate the patterns, and learn how these threats could occur, especially in reconnaissance.

Principal Theme 4: On-Boarding Process

Emulating the advanced countries' successes, Ghana launched a national identification registration scheme as the backbone of the technology initiative for her citizens' security (Stranek-Africa, 2019). The national identification card (NIC) has become the preferred identity card for mobile phone registration. The study discovered that the telecom industry's onboarding process covers mobile phone SIM card registration methods, and leverages a nationwide campaign for mobile subscribers to re-register their SIM cards using the NIC as the valid form of identity card. The implication is that the NIC has additional biometric data embedded, strengthening the security features for the onboarding process. Figure 1, an illustrative overview diagram, provides a simplified interpretation of the onboarding process for mobile money services.

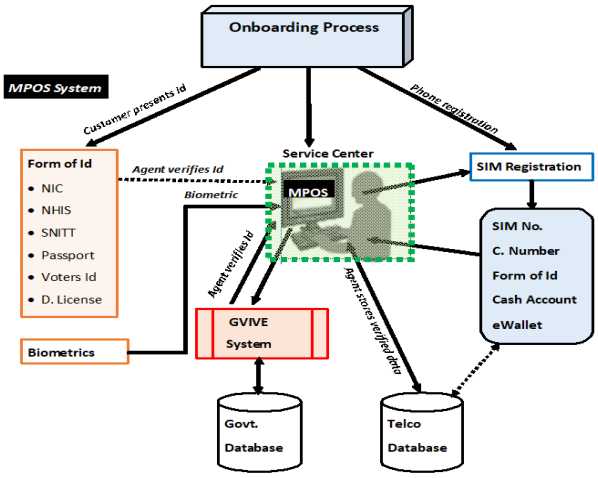

Figure 1: The Onboarding Process Diagram Derived from the Participants' Responses

Registration must reference a SIM Card and Mobile Number and information on a valid Government Issued Identity Card including demographical data like the legal name, date of birth (DOB), Identity Card number, and the next king or heir. In situations where the credentials do not match, the telecom's certified registration manager will authenticate the process by asking security questions to verify the authenticity of the Identity card presented by the subscriber. When the customer and the agent agree to load the money, the initial MoMo sending process begins right after onboarding. All data is stored on the telecom company's data servers as the

background information for the mobile money account.

Principal Theme 5: Phishing Scam Control
Phishing scams stood up as the most severe mobile money services threat ravaging every facet of the MFS business in this study. The menace appeared as a high-tech scam that manifested itself in different ways of fraudulent actions, including deceptive calls, mobile channel extortion, internet extortion, mobile fraud, identity theft, or hacking. The study showed that phishing incidents usually occurred when the scammers tricked subscribers into disclosing their secret PIN codes through a phone call, SMS text messages, or embedded hidden malware in an email link (Asha & KR, 2021). Additionally, fraudsters discovered a means to steal users' credit card sensitive data when they send fake mobile SMS or place calls through impersonation. As identified in this study, the fraud occurred when fraudsters employed social engineering tools like cited phishing tactics to trick mobile subscribers and agents when fraudsters pretended to use valid registered mobile numbers to call their victims (Wrigley, 2018).

Other forms of phishing identified in this study were smishing and vishing attacks when fraudsters used an emotional delusional SMS message to trick users into revealing their mobile money PIN (Maseno et al., 2017). Once executed, the fraudster exploits the existing flaws and sends an SMS to trick the user (victim) into confirming a payment when no money has been transferred.

8. CONCLUSION

The focus of this qualitative exploratory study aimed to explore security methods cybersecurity managers needed to implement to minimize cyber fraud of mobile financial services in developing nations, particularly in Ghana. The exploratory design was best suited because the objective was to capture in-depth information-rich data content. The response to the research question addressed the overarching problem - the lack of efficient methods managers need to implement to minimize cyber fraud in mobile money services. The study's findings have concluded the essence of the theoretical framework describing methods to mitigate cyber fraud as a similitude to the game theory and innovation and adoption of planned behaviors. The implication was a failure to provide an adequate defense to mobile systems proactively. The relay goes to the fraudster or the cyber expert to win the game.

9. RECOMMENDATIONS

The study deduced that the world's economy is increasingly expanding mobile financial services through online and mobile platforms. Consumers deem MFS convenient at any location with a wireless signal. Past research has revealed scant literature on a holistic approach to reducing mobile cash fraud. The rise in cashless transactions through mobile devices is hitting skyrocketing levels in everyday business transactions critical to developing economies. There has been no thorough method to secure mobile financial services to minimize security exposure and prevent fraud, as these threats have caused some providers to lose billions of dollars. USSD and SMS as a mode of transmission for financial data coupled with SS7 protocol present enormous security concerns. GSM architecture has inherent encryption algorithm flaws, and MFS operations lacking adequate internal controls have led to the four recommendations to reduce these threats.

Recommendation 1
The practical implications of this study focus on methods and processes for fraud prevention. The holistic techniques in this study's contribution centered on adequately securing the PIN Code to Mobile Accounts from a practical perspective. Factors affecting the security of the PIN Code depend on three actors mentioned earlier in this document, including cybersecurity experts, agent operators, and subscribers. These factors reflect the practical sense of the game theory with the innovation adoption-behavior model, where the findings of this study clearly articulate the concept of the stringent dichotomy of perpetual cyberwarfare existing between cybersecurity experts' world and cyber fraudsters. The cybersecurity experts must perform their duties in establishing the appropriate security methods mandating strict policies and procedures in mobile network operations. Cybersecurity managers must develop policies involving top managers, agent operators, and subscribers regarding the use of their mobile network. Engaging the subscribers in policy-making could be accomplished through open surveys and customers' feedback.

Recommendation 2
The implications remained on the need to mandate biometric-based identity cards like national identity cards for onboarding and cash withdrawal processes. The risk assessment method embedding threat modeling was a valuable tool for detecting most vulnerabilities and potential threats. A great discovery has

shown that the daily risk assessments conducted within the mobile network infrastructure have been quite helpful. The most critical finding was using encryption technology to protect users' privacy. The study revealed AES encryption algorithm with a key length greater than 128-bits was used. The precise key length of at least 256-bits is recommended as such key length can provide adequate security. Scheduled patches installation must be respected regardless of business profitability impediments. Owing to the evolution of technology in the face of fraudsters' sophistication advancement, cybersecurity managers must retire the use of mobile architectural generation lower than 4G/LTE. Instead, they must deploy a 5G network blended with SDN architecture (Niyaz et al., 2017).

Recommendation 3

The mobile agent operators who are savvy in mobile technology must not take advantage of their customers. Cybersecurity experts must restrict agent operators and affiliated contractors from the administrator access to mobile systems. Restricting agent operators from installing privileges can prevent replay attacks by installing software to withdraw smaller amounts from mobile subscribers' accounts. Prevent manipulating the SMS text by making it read-only when conveying money transfers to subscribers' accounts and prevent extorting customers' mobile money accounts. Agent operators must receive adequate security awareness training to combat phishing scams and to allow agent operators to defend themselves and the entire telecom industry. Management must devise a standard form of identity verification, especially in a cash withdrawal transaction. Strict measures must cover any cash transfers mandating agent operators to collect cash from the sender customer before executing and committing the money transfer process.

Recommendation 4

The subscribers must comply with the "You For Know" program designed to guide customers to protect the privacy of their PIN Code to their mobile money accounts. There was also a discovery that the awareness programs developed by the mobile carriers do not reach even the agent operators, not to mention the subscribers. The subscribers must note that the only security tool for protecting their mobile accounts is their PIN Code, activating the security features on their mobile handsets, and upgrading iOS and Android to mobile application security verification standards (MASVS). The cybersecurity expert could not deliver absolute security protections to their accounts except through the two parties' collaboration.

10. REFERENCES

Akomea-Frimpong, I., Andoh, C., Akomea-Frimpong, A., & Dwomoh-Okudzeto, Y. (2019). Control of fraud on mobile money services in Ghana: an exploratory study. *Journal of Money Laundering Control, 22*(2), 300-317. https://doi.org/10.1108/JMLC-03-2018-0023

Amoroso, D. L., & Magnier-Watanabe, R. (2012). Building a research model for mobile wallet consumer adoption: the case of mobile Suica in Japan. *Journal of Theoretical and Applied Electronic Commerce Research, 7*(1), 94-110. https://doi.org/10.4067/S0718-18762012000100008

Asha, R. B., & KR, S. K. (2021). Credit card fraud detection using artificial neural network. *Global Transitions Proceedings, 2*(1), 35-41. http://www.keaipublishing.com/en/journals/global-transitions-proceedings/

Bank of Ghana. (2020). Summary of economic and financial data. https://www.bog.gov.gh/wp-content/uploads/2020/03/Summary-of-Economic-Financial-Data-March-2020.pdf

Bazen, A., Barg, F. K., & Takeshita, J. (2021). Research techniques made simple: An introduction to qualitative research. Journal of Investigative Dermatology, 141(2), 241-247.

Bettman, J., & Harris, M. (2014). Mobile money: The impact of smartphones on the international remittance market. *Journal of Payments Strategy & Systems, 8*(3), 264-273.

Boateng, K. (2018). Ghana's progress on reaching out to the unbanked through financial inclusion. *International Journal of Management Studies, 5*(2).

Bogdanov, A., Khovratovich, D., & Rechberger, C. (2011). Biclique cryptanalysis of the full AES. Proceedings of theory and application of cryptology and information security. *International Conference on the, in ASIACRYPT 2011: Advances in Cryptography*, 344-371. https://doi.org/10.1007/978-3-642-25385-0_19

Botchey, F. E., Qin, Z., & Hughes-Lartey, K. (2020). Mobile money fraud prediction—A cross-case analysis of the efficiency of

support vector machines, gradient boosted decision trees and naïve Bayes algorithms. *Information,11*(383). https://doi.org/10.3390/info11080383

Brummer, C., & Gorfine, D. (2014).FinTech: Building a 21st-Century Regulator's Toolkit

Burr, W. E. (2003). Selecting the advanced encryption standard. *IEEE Security & Privacy, 99*(2),43-52. https://doi.org/10.1109/MSECP.2003.1193210

Chaeikar, S. S., Yazdanpanah, S., & Chaeikar, N. S. (2021). Secure SMS transmission based on social network messages. International Journal of Internet Technology and Secured Transactions, 11(2), 176-192.

Chironga, M., De Grandis, H., & Zouaoui, Y. (2017). Mobile financial services in Africa: Winning the battle for the customer. *McKinsey & Co. Financial Services*.

Creswell, J. W. (2014). *Research design: Qualitative, quantitative, and mixed methods approach– 4th edition.* Sage Publications.

de Sá, A. G., Pereira, A. C., & Pappa, G. L. (2018). A customized classification algorithm for credit card fraud detection. *Engineering Application and Artificial Intelligence* 72, 21–29.

Editorial Board. (2016). *Perspectives of Qualitative Research Methods.* Words of Wisdom, LLC.

Guma, A., Dida, M. A., & Anael Elikana, S. (2020). Evaluation of key security issues associated with mobile money systems in Uganda. *Information,11*(6),309. http://dx.doi.org/10.3390/info11060309

Guo, J., & Bouwman, H. (2016). An ecosystem view on third party mobile payment providers: A case study of Alipay wallet. *Info,* 18, 56–78.

Gupta, S., Kar, A. K., Baabdullah, A., & Al-Khowaiter, W. A. A. (2018). Big Data with cognitive computing: A review for the future. *International Journal of Information Management*, 42, 78–89.

Hajek, P., & Henriques, R. (2017). Mining corporate annual reports for intelligent detection of financial statement fraud–A comparative study of machine learning methods. *Knowledge-Based System,* 128, 139–152.

IndustryARC. (2019). *Mobile money market – Forecast 2021 - 2026.* Industry Analysis Research Consulting Report Code: ITR 0035. https://www.industryarc.com/Report/15195/mobile-money-market.html

Ingle, S. (2019). Mobile money market — Statistics, growth analysis, trends, demand, competitive landscape to 2023. *Medium*

Kanobe, F., Alexander, P. M., & Bwalya, K. J. (2017). Policies, regulations, and procedures and their effects on mobile money systems in Uganda. *The Electronic Journal of Information Systems in Developing Countries, 83*(1), 1-15.

Khozooyi, N., Tahajod, M., & Khozooyi, P. (2009). Security in mobile governmental transactions. *Second International Conference on Computer and Electrical Engineering, 2*, 168-172.

Kisekka, J. I. (2019). MTN Uganda issues a statement on mobile money fraudulent withdrawals, 2019. https://www.dignited.com/45203/mtn-statement-mobile-money-fraud-withdrawals/

Kolokoltsov, V. N., & Malafeyev, O. A. (2020). Understanding game theory: Introduction to the analysis of many agent systems with competition and cooperation. (p. 3). *World Scientific*

Kyeremeh, H. (2018). Ghana's National Cybersecurity Policy and Strategy (NCSPS): Critique and Comparison with Best Practice

Lee, K., & Narayanan, A. (2021). Security and privacy risks of number recycling at mobile carriers in the United States.

Leedy, D. P., & Ormrod, J. E. (2016). *Practical Research: Planning and Design, 11e*. Published by Pearson Education, Inc.

Lei, Z., Nan, Y., Fratantonio, Y., & Bianchi, A. (2021). On the insecurity of SMS one-time password messages against local attackers in modern mobile devices. In Proceedings of the *2021 Network and Distributed System Security (NDSS) Symposium*.

Levitt, H. M. (2021). Qualitative generalization, not to the population but to the phenomenon: Reconceptualizing variation in qualitative research. Qualitative Psychology, 8(1), 95.

Maseno, E. M., Ogao, P., & Matende, S. (2017). Vishing attacks on the mobile platform in Nairobi County, Kenya*. International Journal Advanced Research Computing and Scientific. Technology,* 5, 73–77.

McSweeney, K. (2018). Motivating cybersecurity

compliance in critical infrastructure industries: A grounded theory study. (10744158 Ph.D.), Capella University.

Mtaho, A. B., & Mselle, L. (2014). Securing mobile money services in Tanzania: A Case of Vodacom M-Pesa. *Int. J. Comput. Sci. Netw. Solut., 2*, 1–11.

Myerson, R. B. (2013). Game theory: Analysis of conflict. *Harvard University Press*.

Naomi Kwetey, D. B. A., Caesar, L., Appiah, D., & Collins Cobblah, M. B. A. (n.d.). Banking the unbanked in Ghana. *SBS Journal of Applied Business Research, 44.*

Naseri, R. N. N. (2021). What is a population in online shopping research? A perspective from Malaysia. *Turkish Journal of Computer and Mathematics Education (TURCOMAT), 12*(4), 654-658.

National Communications Authority. (2020). *Mobile voice subscriptions from January to March 2020*. Communications Industry Statistics. https://www.nca.org.gh/industry-data-2/market-share-statistics-2/telecom-voice/Communications-Industry-Statistics-MV-Q1.pdf

Nicco-Annan, J. (2020). *That's MoMo like it: Everything you need to know about mobile money in Ghana.* WorldRemit. https://www.worldremit.com/en/stories/story/2020/05/28/mobile-money-ghana

NIST. (2020). National institute of standard and technology special publication 800-53, Revision 5. *Natl. Inst. Stand. Technol. Spec. Publ. 800-53, Rev. 5*, 492 pages (September 2020). https://doi.org/10.6028/NIST.SP.800-53r5

Niyaz, Q., Sun, W., & Javaid, A. Y. (2017). A deep learning-based DDoS detection system in software-defined networking (SDN). *EAI Endorsed Transactions on Security and Safety, 4*(12), Article ID 153515, 2017.

Normans Media Ltd. (2017). Mobile money market global key vendors, manufacturers, suppliers, and analysis market report 2022. *M2 Presswire*.

Novelan, M. S., Husein, A. M., Harahap, M., & Aisyah, S. (2018). SMS security system on mobile devices using a tiny encryption algorithm. *In journal of physics: conference series 1007(*1), 012037). *IOP Publishing*.

Nyamtiga, B. W., Anael, S., & Loserian, L. S. (2013). Enhanced security model for mobile banking systems in Tanzania. *Intl. Jour. Tech. Enhancements and Emerging Engineering Research, 1*(4), 4–20.

Osborne, M. J. (2004). *An introduction to game theory (Vol. 3).* Oxford University Press.

Osborne, N., & Grant-Smith, D. (2021). In-depth interviewing. *Methods in Urban Analysis,* 105-125.

Paganini, P. (2016). *SS7 Protocol: How Hackers Might Find You.* InfoSec. https://resources.infosecinstitute.com/topic/ss7-protocol-how-hackers-might-find-you/

Ponnusamy, V., Selvam, L. M. P., & Rafique, K. (2020). Cybersecurity governance on social engineering awareness. *In Employing Recent Technologies for Improved Digital Governance,* 210-236. *IGI Global.*

PR Newswire. (2019). Mobile money market to expand at CAGR of 22% till 2024, rising mobile payments drive growth; says TMR. *Transparency Market Research*. https://doi.org/201902260500PR.NEWS.USPR.IO65412

Ranjan, J., & Foropon, C. (2021). Big data analytics in building the competitive intelligence of organizations. *International Journal of Information Management, 56*, 102231.

Sadgali, I., Sael, N., & Benabbou, F. (2019). Performance of machine learning techniques in the detection of financial frauds. *Procedia Computer Science*, 148, 45–54.

Salahdine, F., & Kaabouch, N. (2019). Social engineering attacks: a survey. *Future Internet, 11*(4), 89.

Saxena, S., Vyas, S., Kumar, B. S., & Gupta, S. (2019). Survey on online electronic payments security. In Proceedings of the *2019 Amity International Conference on Artificial Intelligence (AICAI)*, 746–751

Sekaran, U., & Bougie, R. (2010). *Research methods for business: A skill-building approach, (5th ed.).* John Wiley & Son

Shin, S., Yegneswaran, V., & Porras, P. (2013). AVANT-GUARD: Scalable and vigilant switch flow management in software-defined networks. Proceedings of the *2013 ACM SIGSAC conference on Computer & communications security*, pp. 413– 424.

Singh, G., Gupta, R., Rastogi, A., Chandel, M. D., & Ahmad, R. A. (2012). Machine learning approach for detection of fraud based on SVM. *International Journal of Scientific*

Engineering and Technology, 1, 192–196.

Singh, H. B., & Kumar, G. (2018). Cybercrimes: A proposed taxonomy and challenges. *Journal of Computer Networks and Communications*. https://doi.org/10.1155/2018/1798659

Smith, J. M. (1982). *Evolution and the theory of games.* Cambridge University Press.

Sowmiya, G., & Malarvizhi, S. (2022). Design of Testability Structures with Security for Machine Intelligence-Based Cryptosystem. *SRMIST: SRM Institute of Science and Technology.* Research Square. https://doi.org/10.21203/rs.3.rs-1217671/v1

Stranek-Africa. (2019). *National identification registration will be an exercise in futility – Stranek-Africa.* Fly Multimed Ghana. https://flymultimediagh.com/2019/12/09/national-identification-registration-will-be-an-exercise-in-futility-stranek-africa/

Talom, F. S. G., & Tengeh, R. K. (2019). The impact of mobile money on the financial performance of SMEs in Douala, Cameroon. *Sustainability 12*(1), 183.

Thebftonline.com. (2022). Future of MoMo industry hinges on partnerships - CEO. *Business News* of Friday, 12 August 2022. https://www.ghanaweb.com/GhanaHomePage/business/Future-of-MoMo-industry-hinges-on-partnerships-CEO-1601423

Von Neumann, J., & Morgenstern, O. (1947). Theory of games and economic behavior. (2nd rev. ed.).

Weber, S. H., & Studer, E. (2016). Cybersecurity in the internet of things: legal aspects. *Computer Law & Security Review, 32*(5), 715–728.

Weigel, F. K., Hazen, B. T., Cegielski, C. G., & Hall, D. J. (2014). Diffusion of innovations and the theory of planned behavior in information systems research: A meta-analysis. *Communications of the Association for Information Systems, 34*(1), 619–636.

Wrigley, J. (2018). *Exploring the causes and defenses of Social Engineer in Developing nations: Using Ghana as a Case Study*. Colorado Technical University Doctorate Research Paper (108288880 DCS). https://doi.org/108288880

Yadav, A. K. S., & Sora, M. (2021). Fraud detection in financial statements using text mining methods: A review. In *IOP conference series: Materials science and engineering 1020*(1), 012012. IOP Publishing.

Yao, J., Han, Z., Sohail, M., & Wang, L. (2019). A robust security architecture for SDN-based 5G networks. Future Internet, 11(4), 85.

Yin, D., Zhang, L., & Yang, K. (2018). DDoS attack detection and mitigation with Software-Defined Internet of Things Framework. *IEEE Access, 6,* 24694–24705.