OPEN ACCESS

Scholars International Journal of Law, Crime and Justice
Abbreviated Key Title: Sch Int J Law Crime Justice
ISSN 2616-7956 (Print) | ISSN 2617-3484 (Online)
Scholars Middle East Publishers, Dubai, United Arab Emirates
Journal homepage: https://saudijournals.com

Review Article

A Critical Examination of the Challenges Impeding the Effective Implementation of MTN-Mobile Money Regulations in Cameroon

Eyong Ayuk Andreas[1*]

[1]Ph.D. Candidate, Department of English Private Law, Faculty of Law and Political Science, University of Dschang, Dschang, Cameroon

DOI: 10.36348/sijlcj.2024.v07i07.002 | **Received:** 11.12.2023 | **Accepted:** 19.01.2024 | **Published:** 24.07.2024

***Corresponding author:** Eyong Ayuk Andreas
Ph.D. Candidate, Department of English Private Law, Faculty of Law and Political Science, University of Dschang, Dschang, Cameroon

Abstract

There is no gainsaying that MTN-Mobile Money plays a vital role in the economy of most nations especially the advent of digitalization in the world today. In Cameroon, a plethora of legislations have been enacted and well established institutions at various levels with diverse competences in ensuring compliance with the protection of MTN Mobile Money services. Despite these laws and institutions in place, MTN Mobile Money services have been plaque with numerous challenges which impedes effective implementation. In tandem with this state of affair, the aim of this paper is to explore the challenges faced in enforcing mobile money regulations in Cameroon, examining the key obstacles and their implications for the effective regulation of this sector. Through a content analysis of primary and secondary data, we therefore, uphold that there would be security and certainty in MTN-Mobile Money Services if these challenges are effectively curtailed in Cameroon and the world at large.

Keywords: Critical, Analysis, Challenges, MTN, Mobile Money, Regulation, Cameroon.

INTRODUCTION

With the advent of mobile money as a rapidly growing technology, governments have had to develop efficient policies to regulate it without hampering its development. Mobile money offers a new world of finance - particularly for the unbanked populations of the world. Formal financial services have historically been offered by traditional banking institutions, and the entrance of financial intermediaries and mobile networks into the playing field encourages competition and pushes the boundaries of traditional banking. In the long run, this benefits consumers and the larger economic system. As Di Castri [1], observes, an enabling policy and regulatory framework creates an open and level playing field that fosters competition and innovation, leverages the value proposition of both banks and non-bank providers, attracts investments, and allows providers to focus on refining operations and promoting customer adoption.

Despite the importance of consumer protection, ensuring the safety of customer funds remains one of the biggest challenges faced by mobile money systems and regulators. Globally, mobile money is responsible for transacting close to $700 billion per annum, and many use it as an alternate method of saving or keeping their money safe [2]. In terms of transactions, mobile money networks are most commonly used to make quick transfers over geographically disparate locations, and in areas with high crime rates that increase the risk of holding cash. Essentially, if MNOs are unable to guarantee the safety of their customer's funds, they fail to deliver on their value proposition.

To be successful and gain the trust of customers, mobile money providers need to implement mechanisms that prevent the loss of their funds. Regulators also need to establish policies that require providers to operate safely in the market. Common causes for the loss of customer funds include bankruptcy of the mobile money issuer or imprudent investments using customer funds. In cases where customer funds are managed by a third-party fiduciary, the trustee's solvency can also be a cause for loss. To mitigate these risks, regulators have several tools

[1]Di Castri, (2019), "Mobile Money: Enabling Regulatory Solutions.", p.4.
[2]Mechale, A., (2021). "Mobile Money and Consumer Protection: An Analysis of Regulatory Environments To Enable Mobile Money," Joseph Wharton Scholars. Available at https://repository.upenn.edu/joseph_wharton_scholars/113, p. 21-22.

available to them to protect customer funds. However, there are significant variations in both the availability and implementation of these tools across countries.

Mobile money, the use of mobile phones to conduct financial transactions, has gained significant popularity in Cameroon over the past decade. The growth of mobile money services has provided numerous benefits, including increased financial inclusion and improved access to financial services for individuals who were previously unbanked. However, the rapid expansion of mobile money has also presented regulatory challenges for the government of Cameroon. Ineffective policies and cumbersome regulatory barriers have had a negative effect on the development of mobile money and the expansion of financial inclusion in many new markets. However, the principal categories of factors which tend to discourage the universal adoption of mobile money service are mainly regulatory, infrastructural and those which arise from traditional perceptions [3].

However, this paper aims to explore the challenges faced in enforcing mobile money regulations in Cameroon, examining the key obstacles and their implications for the effective regulation of this sector. These challenges are divided into legal, institutional and socio-economic in nature.

Legal Challenges in the Implementation and Enforcement of Mtn-Mobile Money Regulations

Legal challenges in the implementation and enforcement of regulations for the protection of consumers of MTN Mobile Money in ensuring the sustainability of services offered in Cameroon include the following:

Lack of Regulatory Clarity

One of the primary challenges in enforcing mobile money regulations in Cameroon is the lack of regulatory clarity. The regulatory framework governing mobile money services in the country is complex and fragmented, with multiple government agencies and regulatory bodies involved in overseeing different aspects of the sector [4]. This fragmentation often leads to overlapping mandates, inconsistent interpretation of regulations, and a lack of clear accountability, making it difficult to effectively enforce and monitor compliance with mobile money regulations [5].

Cumbersome Regulatory Conditions in MTN Mobile Money Services

Cumbersome regulatory regimes can also be a factor for the failure of mobile money networks. This problem was identified by a study conducted by the University of Chicago [6]. In a study of 22 countries where mobile money had been introduced between 2005 and 2015, the authors found that heavy regulation is usually fatal to igniting mobile money schemes in a country [7]. Most countries where mobile money failed to reach the critical ignition point necessary for explosive growth had imposed requirements that mobile money systems were established by banks and prohibited MNOs from taking the leading role.

Two main factors explain the rejection of non-bank-led mobile money deployment. They provide limited financial services to customers, contrasting with "full" financial inclusion through the formal banking sector [8]. But this misunderstands the barriers to financial inclusion which mobile money has helped to solve, and how mobile money platforms have provided a pathway to later formal banking inclusion through credit extension, insurance, and savings products.

The more cogent objection is against licensing a non-bank to offer financial services with financial risks, but without being legally subject to prudential oversight. This objection has been neatly surmounted in many countries by requiring a partnership between the (service leading) MNO and one or more fully prudentially regulated banks, where the electronic value in the customers' mobile money accounts is fully or partially backed up in bank accounts [9]. The role of the partner bank is thus only as custodian of the funds and it is not involved in the commercial aspect of the deployment [10].

Lack of Privacy and data security Law

Considerable personal data (i.e. geographical location, passwords and payment transaction information) is transferred during mobile payments, and

[3]Must, B.; Ludewig, K. Mobile Money: Cell phone banking in developing countries. *Policy Matters J.* 2010, *7*, 27–33. See also Rubini, A. *Fintech in a Flash*; Createspace: London, UK, 2017. See also Baganzi, R.; Lau, A.K.W. Examining trust and risk in Mobile Money acceptance in Uganda. *Sustainability* 2017, *9*, 2233 and also Financial Inclusion. *Pakistan Wave 4 Report FII Tracker Survey*; InterMedia: Washington, DC, USA, 2017.
[4]Nkengfack, C. (2019). Mobile Money Regulation in Cameroon: Challenges and Prospects. Journal of Internet Banking and Commerce, 24(2), p. 9.
[5]Ibid p.11.
[6]Evans and Pirchio, (2014), "An Empirical Examination of Why Mobile Money Schemes Ignite in Some Developing Countries but Flounder in Most." SIJLCJ, P.6.
[7]Ibid, p 4
[8]Mechale, A., (2021), "Mobile Money and Consumer Protection: An Analysis of Regulatory Environments to Enable Mobile Money," Joseph Wharton Scholars. Available at https://repository.upenn.edu/ joseph_wharton_scholars/113, p. 15-16.
[9] Ibid.
[10] Aron, "'Leapfrogging': A Survey of the Nature and Economic Implications of Mobile Money.", 76.

is accessible to mobile network operators, application developers, payment processors and merchants (not to mention parties that can also potentially gain illegal access to that data during the payment process) [11]. Consumers do not necessarily know whether, and how, the data is stored, processed and used, which is problematic as they should have control over their personal data. The collection and use of payment data is also an issue because consumers may not agree to their activities being tracked, or their data being shared with third parties.

Like other financial services, mobile money raises issues of privacy and data protection, some of which are addressed by national privacy laws, telecommunications regulation, and financial regulation, but most by everyday business practice. Data in a mobile money transaction may include: Payer and payee IDs, geographic location, time of day, purchased items, and the value of the transaction. MTN MoMo terms and conditions (Mobile money, which is the brand under which Mobile money corporation (MMC) markets Mobile money (MoMo) Services provides that at the opening of the account, the holder must complete the subscription form and provide an identity document including his photograph and all other documents required by MMC. For example, MTN Ghana requires that to apply for a Wallet, Ghanaian citizens with valid ID and documents may apply for a Mobile Money Wallet; while foreigners wanting to benefit from this service may be required to provide evidence of residence, in the form of a resident permit. Also, persons below the age of 18 (minors) can open a Mobile Money Wallet. A person above the age of 18 may however open a MTN Mobile Money Account Wallet to be held in trust for a minor.

After opening the MoMo Account, MMC may require an update of the information or additional items. The holder must provide them. Mobile money providers have internal controls to minimize unauthorized access to consumer information, as well as the loss of customer data. Regulators and mobile money providers need to work together to understand security concerns and maintain the integrity of customer data.

Institutional Challenges in the Implementation and Enforcement of Mtn-Mobile Money Regulations

Institutional challenges in the implementation and enforcement of regulations for the protection of consumers of MTN Mobile Money in ensuring the sustainability of services offered in Cameroon include the following:

Limited Technological Capacity and Infrastructural Resources

Limited technological capacity of regulatory bodies in Cameroon is a major challenge of MTN Mobile Money Services. The rapid advancement of mobile money technology requires regulators to have a deep understanding of the technical aspects of these services [12]. However, many regulatory bodies lack the necessary expertise and resources to keep up with the evolving mobile money ecosystem. This technological gap makes it challenging for regulators to effectively assess compliance, detect and prevent fraud, and address emerging risks associated with mobile money services [13].

On the other hand, limited infrastructure has made it impossible to make mobile money services available to all of the members of the populations of some countries [14]. As has already been noted, cellular coverage tends to be low in many developing countries [15]. As it is particularly low in rural areas, many people are effectively denied access to the advantages which cellular technology provides [16].

Unstable networks and interrupted transmission oblige some users of mobile money services to travel to locations in which their networks are functioning normally to make transactions, thereby incurring additional costs and suffering considerable inconvenience [17]. According to Chimaobi and Chizoba [18], the erratic transmissions of energy by the power supplier also affect users of mobile money services adversely. During blackouts, it is impossible to make

[11] According to Decree n° 2013/0399/PM of February 27, 2013, establishing the modalities of protection for electronic communications of consumers, they are entitled to have their information kept private.
[12] World Bank. (2018). Cameroon Mobile Money Diagnostic: Enabling Mobile Digital Financial Services. Washington, DC: World Bank Group, p.62.
[13] Ibid, P. 65.
[14] International Monetary Fund. *Central African Economic and Monetary Community: Financial System Stability Assessment*; International Monetary Fund: Washington, DC, USA, 2016. See also, John, E.K.; Gwahula, R.; Msemwa, F.M. The influence of perceived risk on the uptake of Mobile Money Services by SMEs operations in Karagwe district, Tanzania. *Int. J. Adv. Eng. Manag. Sci.* 2018, *4*, 703–712.
[15] GSMA. *Enabling Rural Coverage*; GSMA: London, UK, 2018.
[16] GSMA. *Enabling Rural Coverage*; GSMA: London, UK, 2018.
[17] John, E.K.; Gwahula, R.; Msemwa, F.M. The influence of perceived risk on the uptake of Mobile Money Services by SMEs operations in Karagwe district, Tanzania. *Int. J. Adv. Eng. Manag. Sci.* 2018, *4*, 703–712.
[18] Chimaobi, O.V.; Chizoba, O. Boosting small and medium enterprises performance in Nigeria through mobile commerce. *Eur. J. Bus. Manag.* 2014, *6*, 134–141.

transactions (mobile signals blackout), and, in some instances, cellular devices are damaged beyond repair (electricity blackout).

Furthermore, while the success of digital financial service is partly due to the wide infrastructural outreach of MNOs, network coverage is still a hurdle to customer use of such financial services, especially in rural areas where cell network coverage can be lacking, or where coverage may exist, but agent networks may not be present. Network issues have not only meant that money cannot be transferred when needed, but also that money has gone "missing" in the digital void. The infrastructural technology of digital financial service providers does not always seem equipped to deal with these situations. Disruptions to the system can result in not only in phone credit loss and it can influence consumer's views of mobile money with the provider [19].

Also, the fragmented regulatory landscape in Cameroon poses coordination challenges. Multiple government agencies and regulatory bodies are involved in overseeing various aspects of the mobile money sector, leading to overlapping mandates and a lack of clear accountability [20]. Enhancing coordination among these regulatory bodies through the establishment of interagency collaboration mechanisms and the development of a unified regulatory framework can improve the effectiveness of enforcement efforts and ensure consistent interpretation and application of mobile money regulations.

Above all, the capacity of regulatory bodies to effectively enforce mobile money regulations is a critical challenge. Insufficient resources, limited staffing, and inadequate training impede the ability of regulators to monitor compliance, investigate complaints, and take necessary enforcement actions [21]. Strengthening the capacity of regulatory bodies through training programs, increased funding, and collaboration with international partners can enhance their ability to enforce regulations and safeguard the interests of mobile money users [22].

Lack of Trust and Confidence on MTN Mobile Money services (Informal Financial Sector and Traditional Customs)

Cameroon has a large informal financial sector, which poses challenges for the enforcement of mobile money regulations. Informal financial networks, such as rotating savings and credit associations (ROSCAs) and village savings and loan associations (VSLAs), have deep roots in Cameroonian society and continue to be widely used [23]. These informal networks often operate outside the purview of formal financial regulations, making it difficult for regulators to monitor and regulate transactions that occur through these channels [24]. This lack of oversight creates a potential regulatory gap and undermines the effectiveness of mobile money regulations in Cameroon.

Furthermore, significant numbers of members of the populations of developing countries tend not to trust modern technology and prefer to carry cash with them, owing to the degree of control over their transactions which they perceive that doing so provides [25]. For instance, it is not possible to request a refund or to stop a transaction which has already been validated in a mobile money transaction, while it is easy to do so in the case of cash payment in a supermarket. Moreover, in Pakistan for example, no matter the level of education, people still prefer to keep money at home [26].

The Threats of Fraud in Mobile Money Services

A significant challenge in enforcing mobile money regulations in Cameroon is the limited financial literacy among the population. Many users of mobile money services, particularly those in rural areas and low-income communities, may have limited understanding of the risks, rights, and responsibilities associated with these services [27]. This lack of financial literacy makes individuals more vulnerable to fraud and other risks, and it hampers the effectiveness of regulatory efforts [28]. In

[19] M.E. DE BRUIJN, I.C. BUTTER & A.S. FALL (March 2017), "An ethnographic study on mobile money attitudes, perceptions and usages in Cameroon, Congo DRC, Senegal and Zambia", Final report, p. 47.
[20] Fongang, S. (2021). Consumer Protection in Mobile Money Services in Cameroon: A Comparative Analysis. International Journal of Economics, Commerce and Management, 9(2), 128-137.
[21] Nkengfack, C. (2019). Mobile Money Regulation in Cameroon: Challenges and Prospects. Journal of Internet Banking and Commerce, 24(2), 1-14.
[22] World Bank. (2018). Cameroon Mobile Money Diagnostic: Enabling Mobile Digital Financial Services. Washington, DC: World Bank Group.
[23] Kasekende, L. (2019). The Role of Mobile Money in Financial Inclusion: The Case of Cameroon. African Journal of Economic Review, 7(2), 1-18.
[24] Kasekende, L. (2019). The Role of Mobile Money in Financial Inclusion: The Case of Cameroon. African Journal of Economic Review, 7(2), 1-18.
[25] John, E.K.; Gwahula, R.; Msemwa, F.M. The influence of perceived risk on the uptake of Mobile Money Services by SMEs operations in Karagwe district, Tanzania. *Int. J. Adv. Eng. Manag. Sci.* 2018, *4*, 703–712.
[26] Financial Inclusion. *Pakistan Wave 4 Report FII Tracker Survey*; InterMedia: Washington, DC, USA, 2017.
[27] Nkengfack, C. (2019). Mobile Money Regulation in Cameroon: Challenges and Prospects. Journal of Internet Banking and Commerce, 24(2), 1-14.
[28] World Bank. (2018). Cameroon Mobile Money Diagnostic: Enabling Mobile Digital Financial Services. Washington, DC: World Bank Group.

this direction, fraud may occur to a consumer of mobile money services. Consumer-affecting fraud types vary from one market to another. The common risks to which consumers are exposed in mobile money ecosystem are: identity theft, false promotions, phishing, or social engineering scams, overcharging for transactions, Loss from erroneous transfers.

Identity Theft

The term identity theft is defined as the fraudulent practice of using another's person name and personal information in order to obtain credit, loans, etc [29]. It can be used for everything from cheque forgery and the use of stolen credit cards to sophisticated scams in which an impostor adopts other people's identity to gain access to their assets. Concerning mobile money, identity theft can arise from fraudulent/offline SIM swaps that transfer the mobile wallet account from the customer's SIM to the fraudster's SIM, enabling the fraudster to gain access to the consumer's mobile wallet and bank account.

Employees also engage in identity theft/fraud by accessing and exploiting customer information without authorization. Many incidents of this type of fraud have been reported in the news media across other African countries. Fraud situations for mobile network operators (MNOs) can be high; yet because of MNOs non-disclosure, the extent of fraud with mobile money is unknown.

False Promotions, Phishing, or Social Engineering Scams

Phishing is the fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information such as passwords and credit card numbers [30]. Spamming which is sending unsolicited messages, especially advertising, directed at the text messaging or other communications services of mobile phones. Fraudsters through impersonating providers and advising customers they won a prize in a promotion and to send money to the fraudster's number to claim the prize.

Unfair Commercial Practices

According to the Unfair Commercial Practices Directive, the legality of a commercial practice that is not banned outright can be assessed by evaluating it against specific legal criteria. The fairness or unfairness of a commercial practice is assessed against the benchmark of an average consumer (i.e. a reasonably well-informed, observant and circumspect consumer). However, certain commercial practices across EU are always prohibited (e.g. false prize winning, bait advertising). One of the examples of unfair commercial practices related to mobile payments is misleading advertising leading to unexpected charges for the consumers.

A recent case was that of certain in-app purchases advertised as free. Another unfair practice is a hidden payment obligation. For instance, to access free trial versions of cloud computing services, consumers may be asked to provide their credit card details; upon expiration of the trial period, they are automatically charged for the service without their explicit consent. Similarly, the practice of automatic contract or subscription renewal may result in consumers being charged for products or services they may not have wanted.

Also, mobile money remains heavily regulated [31]. In some instances, stakeholders in the traditional banking sector tend to perceive the new system as a threat to the hegemony which they have maintained [32], and do not welcome the prospect of their services being superseded or supplanted by innovative contemporary ones [33].

The pressure which commercial banks are placing upon the central banks of their countries leave them with two possible courses of action: continue with the status quo and retard economic growth as a consequence of stifling the growth of SME sectors or liberalize and permit newcomers to the financial sectors of their countries to boost national economies by providing services which significantly increase the financial performance of SMEs [34]. This pressure is because of the fact that only commercial banks are allowed to issue electronic money [35], and the mobile network operators own the telecommunication infrastructures and technologies to deploy the platform.

False Promotions

This is a new tactic devised by fraudsters. Fraudulent customers send fake SMS to agents either from their own handsets or generated from computers.

---

[29] COBUILT Advanced English Dictionary, Copyright Harper Collins Publishers.
[30] 80 Cf. English Oxford living Dictionaries, website: htttpenglish.en.oxforddictionaries.com.
[31] Rubini, A. *Fintech in a Flash*; Createspace: London, UK, 2017. See also, Must, B.; Ludewig, K. Mobile Money: Cell phone banking in developing countries. *Policy Matters J.* 2010, *7*, 27–33.
[32] Must, B.; Ludewig, K. Mobile Money: Cell phone banking in developing countries. *Policy Matters J.* 2010, *7*, 27.
[33] Amponsah, E.O. The advantages and disadvantages of Mobile Money on the profitability of the Ghanaian banking industry. *Texila Int. J. Manag.* 2018, *4*, 1–8.
[34] Baganzi, R.; Lau, A.K.W. Examining trust and risk in Mobile Money acceptance in Uganda. *Sustainability* 2017, *9*, 2233.
[35] BEAC. Etat des Systemes de Paiement par Monnaie Electronique Dans la CEMAC. Available online: https://docplayer.fr/88945930-Etat-des-systemes-de-paiement-par-monnaie-electronique-dans-la-cemac.html (accessed on 28 December 2018).

Or they lured customers to authorize cash out transactions with the claim of winning mobile money promotion.

Fortuitous Scam

Scamming refers to irrelevant or unsolicited messages sent over internet, typically to a large number of users, for the purposes of advertising, phishing, spreading malware, etc. Firstly, fraudsters call to dupe customers under the pretext of delivering goods from abroad. Also, some fraudsters call and ask for specified amounts to be deposited into a mobile money account, in exchange for goods from relatives or friends from abroad.

To address these issues, there is a need for comprehensive financial education programs that promote awareness and understanding of mobile money services among the population.

Cyber-Insecurity and Fraud in MTN Mobile Money

The increasing reliance on mobile money services in Cameroon has also led to an escalation in cyber security risks and fraud [36]. Mobile money platforms are attractive targets for cybercriminals, who exploit vulnerabilities in the system to gain unauthorized access, steal funds, or engage in identity theft [37].

One type of fraud is a "man in the middle" attack that involves the attacker placing himself or his malicious tools between the victim and a valuable resource, e.g. a banking website or an Email account. For instance, an attacker could configure a wireless device to act as a Wi-Fi hotspot in a public area, such as an airport or coffee shop, giving it a name which resembles one commonly used. When users connect to the 'router' and access sensitive sites such as online banking or e-commerce sites, the attacker is able to capture their credentials for later use. With constant development of new techniques for fraud besides the better known phishing scams to access sensitive consumer data, the danger of fake shops proposing products online and identity theft techniques cyber security will have to evolve continuously.

With the growth of the Internet of things, ever more devices will have access to the internet and to financial service accounts and credentials. Cloud services are becoming an attractive target for cyber-criminals. According to some predictions for 2015, attacks on mobile platforms through malicious links and applications are to be expected and point-of-sale malware could become one of the most common methods of stealing data and money [38].

Ensuring robust cyber security measures and fraud prevention mechanisms is crucial for maintaining trust and confidence in the mobile money ecosystem. Regulators need to work closely with mobile money providers to implement robust security protocols, conduct regular audits, and enhance fraud detection and prevention mechanisms.

Lack of Collaboration and Coordination between Agents and Customers

Users of mobile money highlighted certain complaints concerning the agents providing the services. Agents play a key role in promoting mobile money services, keeping the customer informed about how services work and removing worries when things go wrong. Negative experiences can discourage individuals from using the services. Problems with float, for example, influence user perceptions of digital financial services. Some agents frequently run out of float or cash with which to complete transactions, forcing customers to search for another agent or return later. This tarnishes the reputation of digital financial services providers as a whole, and not just that of the single agent in question.

1. Agents who ask for the customer's personal identification number (PIN). (Even where this may not necessarily have been done to defraud customers, it makes consumers more vulnerable to fraud risks). This is why MNO always sends messages to customers to not give their PIN to any agent.
2. Overcharging for transaction by agents who defraud customers by charging unauthorized fees through over the-counter (OTC) transactions such as direct deposits are illegal in a number of countries or charging for normal deposits, which are typically free.
3. Provider impersonation by fraudsters who call consumers purporting to represent the provider and may then induce them to reveal their PIN or other personal information about their mobile money accounts, which can be used to defraud the customer.
4. Loss from erroneous transfers to unintended recipients who refuse to refund the money is another major issue. Fraud can be committed during network down time, mainly through offline SIM swaps and over the-counter (OTC) transactions that can be verified and reconciled only later when the network connection is restored. When the service is unavailable for a

[36] World Bank. (2018). Cameroon Mobile Money Diagnostic: Enabling Mobile Digital Financial Services. Washington, DC: World Bank Group.

[37] Kasekende, L. (2019). The Role of Mobile Money in Financial Inclusion: The Case of Cameroon. African Journal of Economic Review, 7(2), 1-18.

[38] Jana VALANT (June 2015), "Consumer protection aspects of mobile payments", EPRS (European Parliamentary Research Service).

while, this can result in delays in effecting cash in/cash out transactions, which denies customers to access to their own money.

Dormant Assets in Electronic Wallets or Electronic Purses

Money can be stored in electronic wallets or electronic purses, in the form of credit on mobile phones or in apps. The aggregate value of these otherwise relatively small amounts could be considerable, especially with the increase of mobile commerce. One of the non-regulated issues related to mobile payments is dormant assets, i.e. the money to which consumers lose access. The money is still on the platform used for mobile payments but is not being used by the user anymore. As the access codes are normally known only to the owner, recuperation of the amount kept on a specific mobile payment platform is obvious, that is, when you lose your phone your MM account is not missing. You can retrieve it. This can happen for a number of reasons.

One would be the death of the owner of the account or device, but other reasons could also be the termination of the mobile phone number account etc. But the problem now is what happens to the money stored in the MM account?

Lack of Monitoring and Limited Enforcement Mechanisms

Mobile money agents play a crucial role in the provision of services, as they are responsible for cash-in and cash-out transactions and act as intermediaries between customers and mobile money providers [39]. However, ensuring compliance among these agents is a challenge in Cameroon. Some agents may engage in fraudulent practices, such as unauthorized transactions or charging excessive fees, which can harm consumers and undermine the integrity of the mobile money ecosystem [40]. Strengthening agent monitoring and enforcement mechanisms, including regular inspections and penalties for non-compliance, is essential to address this challenge.

As aforesaid, mobile money services are vulnerable to various risks, including fraud, unauthorized transactions, and inadequate dispute resolution mechanisms. Ensuring adequate consumer protection requires robust regulations and effective monitoring and enforcement mechanisms [41]. However, the current regulatory framework in Cameroon lacks comprehensive consumer protection provisions, and enforcement efforts are often hampered by limited resources and capacity constraints thus, making consumer protection a critical challenge in enforcing mobile money regulations in Cameroon.

It is also important to note here is that while the "light" regulation of digital financial service (DFS) is one of the main culprits behind the lack of customer protection for DFS users, it is also seen as one of the factors behind the mobile money success story. The relative anonymity it provides and perceived lack of traceability are what seem to make DFS particularly interesting for those in the informal sector and/or for those reluctant to rely on more formal financial institutions. The registration of numerous SIM cards under a false name/ID card render transactions anonymous, to a certain extent, as there is no connection between the person officially linked to the SIM card and to the individual carrying out the transaction.

Our researchers in DRC and Cameroon reported numerous instances where the mobile phone agent used either his own ID card or that of a random person he had lying around to register a customer's SIM card [42].

Risk of Solvency of the Mobile Money Issuer

In the event that the issuer of a mobile money service becomes bankrupt, creditors can attempt to claim customer funds to settle debts. Placing customer funds in a separate trust account can help mitigate this risk by ring-fencing customer funds from other assets held by the issuer. However, the liability of trust accounts and the process for establishing an account vary across contexts.

Though trusts are an effective way to safeguard funds in theory, in practice they can still be at risk of co-mingling with the issuer's assets. The primary reason for this is that the issuer often has direct access to the funds stored in the trust. For example, a mobile money issuer may establish a trust to maintain customer funds, but still use some of the customer funds to make investments without the knowledge of the customers. In such cases, the customer funds are still at risk of loss. The use of a third-party trust can help address this challenge and has been implemented successfully by M-Pesa in Kenya.

In the case of Kenya's M-Pesa system, the issuer (Safaricom) does not receive the customer funds. Instead, it is paid directly to another firm, called the 'M-Pesa Holding Company' (MPHC). The MPHC stores

[39] Fongang, S. (2021). Consumer Protection in Mobile Money Services in Cameroon: A Comparative Analysis. International Journal of Economics, Commerce and Management, 9(2), 128-137.

[40] Ndi, G. (2020). The Regulation of Mobile Money in Cameroon: Challenges and Opportunities for CrossBorder Services. International Journal of Economics, Commerce and Management, 8(2), 109-121.

[41] Fongang, S. (2021). Consumer Protection in Mobile Money Services in Cameroon: A Comparative Analysis. International Journal of Economics, Commerce and Management, 9(2), 128-137.

[42] M.E. DE BRUIJN, I.C. BUTTER & A.S. FALL (March 2017), "An ethnographic study on mobile money attitudes, perceptions and usages in Cameroon, Congo DRC, Senegal and Zambia", Final report, p. 59-60.

customers' funds in a trust account with the Commercial Bank of Africa. Under this system, Safaricom facilitates the service and mobile money transactions. However, the MPHC plays the role of handling all the payments under M-Pesa. Safaricom - the issuer of the mobile money service - does not receive, store, or manage any customer funds from mobile money [43].

Additionally, the Central Bank of Kenya for example, has the authority to monitor the MPHC's management of the trust account. Tanzania also employs a similar system. The mobile money issuer is required to establish a separate legal entity that forms and manages a trust account. The corporate structure and management of the separate entity is evaluated and approved by the Bank of Tanzania [44]. It has to submit monthly reports on the operation of the trust to the Bank of Tanzania as well as comply with any additional requirements set forth by the bank. Many countries with mobile money networks recognize the need to prevent commingling of customer funds with the company assets [45]. However, not all of them have an explicit requirement for using trust funds. Policies involving a trust account managed by a third party to handle customer funds have several benefits. Primarily, they ensure that the funds are kept separate from the issuing company's assets. This prevents direct access and makes it difficult to use the funds elsewhere. Second, they enable improved regulation from the government. Instead of dealing with the issuing company, the government can now directly supervise the third-party firm when addressing risks related to the customer funds. Lastly, depending on the fiduciary policies in place, placing customer funds in a trust managed by a commercial bank can help protect them in cases of the solvency of the trustee bank as well.

Problem of Solvency of the Third-Party Fiduciary

Although trust accounts can help mitigate the risk of commingling customer funds with company assets, there are still additional risks posed to customer funds that need to be addressed. Most trust accounts employed by nonbank mobile money issuers are placed in commercial banks. A prominent, but inaccurate, view is that such funds are completely protected [46]. One reason may be that banks are usually subject to heavy capital requirements and regulatory oversight. In developed countries, banks usually receive deposit insurance and other government insurance.

However, in recent years this view has come under examination. This is because many developing countries do not have deposit insurance. Moreover, even in those countries that does have deposit insurance; policymakers have realized that this may not protect customers' funds from the institutional stress of the bank in which such funds are stored [47]. Funds from individual customers are often kept in a pooled account which is treated as a single account for the purposes of deposit insurance. In the event of institutional stresses such as bankruptcy, customers are not guaranteed the entire value of their funds.

A good example is seen when M-Pesa was first established in Kenya. As a result, deposits were protected under the Deposit Protection Fund (DPF) which was designed for individual bank account holders. The DPF provides insurance on a maximum of 100,000 in Kenyan Shillings, which amounts to $1,300. With millions of users, this meant that M-Pesa customer funds were virtually unprotected in the event of a bank failure [48]. In recognition of this weakness; the Kenyan government enacted the Kenya Deposit Insurance Act (KDI Act) in 2012 to protect mobile money users. According to the KDI Act, the deposit held in trust by the trustee for each beneficiary (mobile money user), shall be deemed to be a separate deposit where the trustee is acting for two or more beneficiaries [49]. This model, borrowed from the US Federal Deposit Insurance Corporation (FDIC) is known as pass-through deposit insurance.

Under the pass-through deposit insurance model, the deposit insurance provider acknowledges that under certain circumstances, funds that are combined and held in a single account may be better characterized as a number of smaller accounts for the purpose of deposit insurance protection [50]. The following conditions must be met for the account to viable for pass-through deposit insurance [51].

i. The agency or custodial relationship must be disclosed in the account records of the insured depository institution;
ii. The identities and interests of the actual owners must be disclosed in the records of the depository institution or records maintained by the custodian or other party; and
iii. The deposits actually must be owned by the named owners and not by the custodian.

[43] Greenacre, "Regulating Mobile Money: A Functional Approach",11.
[44] Tanzania National Payment Systems Acts, 23.
[45] Mechale, A. (2021). "Mobile Money and Consumer Protection: An Analysis of Regulatory Environments to enable Mobile Money," Joseph Wharton Scholars. Available at https://repository.upenn.edu/joseph_wharton_scholars/113, p. 23.
[46] Ibid, p.24-25.
[47] Greenacre, "Regulating Mobile Money: A Functional Approach", 15.
[48] Jack and Suri, "The economics of M-PESA.", 10.
[49] See the Kenya Deposit Insurance Act, Article 29.
[50] Grossman, "Safeguarding Mobile Money: How providers and regulators can ensure that customer funds are protected.", 23.
[51] FDIC, New General Counsel's Opinion No.8

Despite the apparent effectiveness of pass-through deposit insurance at protecting customer funds, it is not a very common policy - especially among countries with high levels of mobile money adoption. According to a 2018 survey conducted by the International Association of Deposit Insurers, only 30% of countries have adopted pass-through deposit insurance [52].

Lack of Interoperability between Different Mobile Payment Options

Interoperability is defined as the possibility for customers to operate as a 'walled garden', meaning that transactions can only be performed between users of the same system, i.e. a user can only transfer electronic money to another user of the same mobile money deployment. It is also defined as a situation in which payment instruments belonging to a given scheme may be used in systems installed by other schemes. As technology advances rapidly and options for mobile payment increase, lack of interoperability (including cross-border) between service providers is an issue.

A lack of interoperability has been highlighted as a major barrier to the development of the mobile money market. The strongest reason for enabling interoperability is the dramatic increase in mobile money transactions that will result. Transaction volume in any network is proportional to and driven by the number of interconnections possible between subscribers [53]. Better interoperability would provide consumers with more flexible payment options (better switching between different services and providers), leading to an increase in the number, speed and volume of mobile transactions. Better financial inclusion could be another benefit of more accessible and flexible services for consumers [54].

Interoperability would give mobile money service providers the opportunity to increase the volume of digital transactions, improve the sustainability of mobile money services and contribute to an open digital financial ecosystem which promotes financial inclusion. Building an effective interoperable environment is going to require service providers to engage with policy makers and regulators. The policy maker should act as a facilitator, helping providers to create the road map that they will be primarily responsible for designing and implementing. Their first focus area is Account-to-Account (A2A) interoperability. A2A interoperability in mobile money may create strong positive network effects between banks, which could be expected to apply also for mobile money [55].

Risks of Money Laundering and Terrorism Financing

Mobile money services are currently being rolled out in a number of markets around the world. There is concrete evidence to suggest that these services improve access to formal financial services in developing countries. However, the expansion of these services arouses fears that they may be used for the purposes of money laundering and terrorism financing (ML/TF). Although there have been very few cases of ML/TF up until now, mobile money systems remain susceptible to being used for these purposes in the future (in the same way that other formal financial services are currently being targeted).

The risks of money laundering and terrorism financing linked to mobile money transactions are mainly due to failings in the management systems implemented by financial institutions and their respective partners for these instruments. These risks can be classified into two groups: those linked to customer identification and those linked to carrying out transactions at each link in the chain of stakeholders.

Risks Linked to Customer's Authenticity and Identification of Documents

The risk of money laundering and terrorism financing is increased in the sub-region in that individuals can easily use false identity documents. The lack of an effective mechanism for mobile telephone operators to verify the authenticity of identity documents is a major obstacle to the prevention of these risks, especially because for many mobile money operators, mobile money can be used after the customer is identified, not after the authenticity of the identity document has been verified.

In these organizations, it is often the case that a copy of the identity document is presented, thus rendering it impossible to verify the authenticity of the original identity document. As such, the ability for individuals to move from one country to another in the absence of a sub-regional database for identifying individuals may increase the chance of these risks occurring. The free movement of people between the countries of the sub-region would appear to constitute a risk factor.

Risks of Money Laundering and Terrorism Financing Linked to Customers

This risk may arise in the form of a traditional transfer with a criminal origin or destination (for example, financing terrorism). Although real documentary proof may be used at the time of

[52]"Deposit Insurance and Financial Inclusion: Current Trends in Insuring Digital Stored Value Products.", 14
[53]Ovum Research (2010), Mobile Money in Emerging Markets.
[54]Talla Lele Stephane (2018), "The Protection of Consumers in Electronic Money Institutions: The Case of Mobile Money" Dissertation, Post Graduate Diploma (DIPET II) in Law, University of Buea, P.35.
[55]Ibid, 36.

registration, false information may also be presented. The act of depositing money into the account can also be used to recycle fraudulently obtained funds via the use of stolen bank cards or credit cards (which can be considered to be a 'placement' process). Transactions can also be used to transfer funds between accomplices, or to transfer them to other countries with less stringent AML/CTF laws, where the funds can be used to finance other criminal activities. This process is accompanied by cash withdrawal of the amounts to be used or transferred by other methods [56].

Risks Linked to Carrying Out Transactions by Retailers

Retailers may receive substantial amounts in the form of payments and include them as legitimate proceeds of their business (thus forming part of the process of integration of funds). Retailers may be criminals themselves, swindling their customers, or use their business as a front for laundering the proceeds of their accomplices' activities, who pass themselves off as customers [57].

Risks Linked to Agents, Intermediaries and Retail Partners

These stakeholders occupy a strategic position in the mobile money services payment cycle: loading cards via cash payments, operating purchase or withdrawal points, and also selling telephones that may be used for transactions. These people are therefore able to falsify their records, to ignore suspicions that should otherwise be reported, or simply form a weak link in the chain by not carrying out their role with all due diligence [58].

Risks from Cross-Border Payments

The cross-border nature of mobile money transactions poses additional challenges for regulation and enforcement of MTN Mobile Money regulations. Cameroon shares borders with several neighboring countries, and mobile money services often facilitate cross-border remittances and trade [59]. Regulating cross-border transactions requires close collaboration and information sharing between regulatory bodies across different jurisdictions [60]. The lack of harmonization and coordination among regulatory bodies in the region can lead to gaps in enforcement, making it challenging to effectively regulate mobile money services operating across national borders.

Worthy of note is that, cross-border payments may be used to move money from criminal activity from its original jurisdiction to another jurisdiction in which it can be used to finance other criminal activities, be withdrawn, or sent on to yet another jurisdiction. The cross-border movement of funds makes authorities' searches more difficult and helps to hide the purpose of the transfer. This type of payment is therefore an additional source of risk [61].

Risks of Money Laundering and Terrorism Financing Circumvention via International Transfers

As mobile telephone operators move towards issuing electronic money through VISA-type payment cards to settle transactions and withdraw cash from bank automated distribution machines (ATMs), this may open the door to international transfers intended to launder money and finance terrorism. This also does not take into account that such international transfers would have an effect on the foreign exchange reserves of States in the sub-region [62].

CONCLUSION AND THE WAY FORWARD

Enforcing mobile money regulations in Cameroon is a complex and multifaceted task. The challenges discussed in this chapter, including the lack of regulatory clarity, limited technological capacity, the presence of an informal financial sector, inadequate consumer protection, and the complexities of cross border transactions, highlight the need for a more comprehensive and coordinated approach to regulation. Addressing these challenges requires collaboration among government agencies, regulatory bodies, mobile money operators, and other stakeholders to develop robust regulatory frameworks, enhance technological capacity, and strengthen consumer protection measures. By overcoming these challenges, Cameroon can ensure the sustainable growth and development of its mobile money ecosystem while safeguarding the interests of users and promoting financial inclusion.

Although its importance is affected by factors related to regulation, infrastructures and customs, Mobile Money appears to be the solution to the multiple

[56] Mechale, A. ,(2021). “Mobile Money and Consumer Protection: An Analysis of Regulatory Environments to enable Mobile Money," Joseph Wharton Scholars. Available at https://repository.upenn.edu/joseph_wharton_scholars/113, p. 40.

[57] Mechale, A., (2021). "Mobile Money and Consumer Protection: An Analysis of Regulatory Environments To
Enable Mobile Money," Joseph Wharton Scholars. Available at https://repository.upenn.edu/joseph_wharton_scholars/113, p. 45.

[58] Mechale, A. (2021). "Mobile Money and Consumer Protection: An Analysis of Regulatory Environments to enable Mobile Money," Joseph Wharton Scholars. Available at https://repository.upenn.edu/joseph_wharton_scholars/113, p. 39.

[59] Ndi, G., (2020). The Regulation of Mobile Money in Cameroon: Challenges and Opportunities for Cross Border Services. International Journal of Economics, Commerce and Management, 8(2), 109-121.

[60] Ibid

[61] Ibid, P.41.

[62] Ibid, p. 44.

problems, namely, liquidity, means of payments, debt collection, working capital and financing. Its adoption and usage in their day-to-day activities have had a positive impact on their performance, as shown by many scholars.

The rapid growth of mobile money particularly in regions without access to formal financial services has positioned it as one of the most successful financial innovations of the twenty-first century. Though many are optimistic about the opportunities for financial inclusion that mobile money offers, there are many challenges it has yet to overcome before it can achieve its full potential. Cumbersome regulatory regimes are chief among these challenges. Despite a plethora of positive evidence that points towards the benefits of mobile money, we find that most policy regimes in emerging countries are either hesitant or unprepared to accommodate mobile money.

Nonetheless, certain countries have been able to create environments conducive for the growth of mobile money while simultaneously ensuring the protection of customer data and funds. With the use of mobile money regulatory index constructed by the GSMA, we find that consumer protection is the most important predictor of the number of mobile money users. This finding is contextualized only to sub-Saharan Africa as a region dominated by emerging economies. An important caveat is that while enabling regulation can contribute to the success of mobile money, it is also possible that the already existent success of mobile money prompted the development improved regulation. Though we are unable to address this issue due to a lack of readily available data, it provides strong evidence for further research into the specific causal relationship between consumer protection and mobile money.

On this strand of reasoning, we therefore, recommend that, the government should create an enabling policy and regulatory framework on Mobile Money. With the advent of mobile money as a rapidly growing technology, governments have had to develop efficient policies to regulate it without hampering its development. Mobile money offers a new world of finance particularly for the unbanked populations of the world. Formal financial services have historically been offered by traditional banking institutions, and the entrance of financial intermediaries and mobile networks into the playing field encourages competition and pushes the boundaries of traditional banking. In the long run, this benefits consumers and the larger economic system.

Also, MNO provide an effective customer support to help customers with questions about the service and problems with transactions via phone, SMS, or in-person (such as visiting an agent or operator retail location). Effective support is support that is available whenever a customer has a problem; accessible from wherever a customer might be at that moment; and resolves the problem in a reasonable amount of time.

Ensure a reliable mobile network: A reliable mobile network is a critical component of a mobile payment service, as customers have much less patience for transmission problems when they impact financial transactions. Therefore, access to a reliable network, either an organization’s own or a partner’s is critical, particularly as reliability among mobile networks in emerging markets can vary considerably.

Furthermore, we recommend for a standardized regulatory framework to set the formalities in creating a Mobile Money account. This is because, one of the very challenging issues in mobile banking is ‘Know Your Customer’ regulations (KYC). Under KYC regulations, a customer has to establish his or her identity before using the service. Should the same documents used in the opening of the bank account be used in the opening of mobile account? This is a question which is still unanswered in the mobile banking industry. So far, in most countries where mobile banking is successful, there is no agreed document that could be used to meet KYC requirements. In the ‘non-bank based model’ of mobile banking, the process of opening mobile account does not require much information on the customer. The CEMAC sub region does not have a unifying Regulation on the registration of SIM cards. This thus amplify the complexity in the registration and usage of SIM cards in Mobile Money transactions within the sub region and in mitigating the risk of fraud or dubious dealings that may emanate from the use of SIM cards in Mobile Money transactions within the sub region. We therefore called the attention of the sub regional legislator to this effect to see into it that there exists such a regulation given the borderless nature of e-banking and electronic commerce.