KENYA BANKERS ASSOCIATION

One Industry. Transforming Kenya.

WPS/02/14

Consumer Protection for Mobile Payments In Kenya: An Examination Of The Fragmented Legislation and The Complexities It Presents For Mobile Payments

Joy Malala

KBA Centre for Research on Financial Markets and Policy
Working Paper Series

7

KENYA BANKERS
ASSOCIATION
One Industry. Transforming Kenya.

Working Paper Series

Centre for Research on Financial Markets and Policy

The Centre for Research on Financial Markets and Policy was established by the Kenya Bankers Association in 2012 to offer an array of research, commentary, and dialogue regarding critical policy matters that impact on financial markets in Kenya. The Centre sponsors original research, provides thoughtful commentary, and hosts dialogues and conferences involving scholars and practitioners on key financial market issues. Through these activities, the Centre acts as a platform for intellectual engagement and dialogue between financial market experts, the banking sector and the policy makers in Kenya. It therefore contributes to an informed discussion that influences critical financial market debates and policies.

The Kenya Bankers Association (KBA) Working Papers Series disseminates research findings of studies conducted by the KBA Centre for Research on Financial Markets and Policy. The Working Papers constitute "work in progress" and are published to stimulate discussion and contribute to the advancement of the banking industry's knowledge of matters of markets, economic outcomes and policy. Constructive feedback on the Working Papers is welcome. The Working Papers are published in the names of the author(s). Therefore their views do not necessarily represent those of the KBA.

The entire content of this publication is protected by copyright laws. Reproduction in part or whole requires express written consent from the publisher.

© Kenya Bankers Association, 2013

Consumer Protection for Mobile Payments In Kenya: An Examination Of The Fragmented Legislation and The Complexities It Presents For Mobile Payments

Joy Malala*

Abstract

Innovation has been at the forefront of development in Kenya, primarily through the integration of mobile telephony and retail financial services. Mobile payments have transformed the way financial services have been delivered in Kenya, through bringing a large number of 'unbanked' and 'under banked' [1] persons into the financial realm. These new technologies have almost always outpaced governments' regulatory responses to them. The lack of specific legislation in this area has consequently left the Kenyan regulatory environment open to various risks to consumers. As mobile payments comprise both banking and telecommunications activities, differing perspectives exist on the appropriate regulatory framework as well as which authority should regulate it. To enhance the potential benefits from innovations in this area, governments need to make complementary adjustments to domestic banking and financial regulations by offering specific regulation for mobile payments. In so doing, certain questions should be asked in establishing a strong consumer protection regime as the mobile payments system has brought forth new entrants and various stakeholders. Among these questions include whether the stored value held in banks by consumers is a deposit, therefore subject to bank supervision, oversight and protection. Therefore this paper discusses consumer protection as a major justification for establishing a specific and appropriate regulatory framework for mobile payments in Kenya.

[1] The 'unbanked' and the 'under banked' will be used in this paper to refer to persons who do not have a bank account or those who rely on alternative financial services. See, "Tapping the Unbanked Market" Symposium". Federal Deposit Insurance Corporation (FDIC) <http://www.fdic.gov/news/conferences/TUM_bio.html> accessed 3 September 2013.

* University of Warwick, UK

Introduction

This paper aims to discuss the risks to consumers due to a lack of an established regulatory framework for mobile payments. It will do so by first, identifying the different players in the mobile payments chain, then, presenting the existing framework through which these players are currently operating. It will then discuss the gaps that have been left by the current regulatory framework where consumer protection issues have not been adequately addressed.

The paper will discuss the risks that consumers are exposed to as a result of these gaps. This will be done through a critical assessment of the consumer protection instruments currently relied upon and the limitations that these instruments have in ensuring consumers of mobile payments are protected. Legal frameworks applicable to mobile payments may be insufficiently defined to clearly allocate rights and obligations between consumers and mobile network operators or banks in the event of operational errors incidents of theft or fraud or other unforeseen problems. This paper will finally propose a reform agenda for consumer protection through articulating some policy recommendations that will aid the establishment of a regulatory framework for mobile payments.

Banking in many developing economies such as Kenya , has and continues to be considered the business of the rich who can afford the regular and expensive fees charged by branches, many of which are few and far between. As a result, there has been very little incentive for banks to serve the unbanked mainly due to the significant costs of establishing branch networks and the right margins associated with banking the poor. In 2008 Kenya had a stable growing banking sector that appeared to have avoided most of the rippling effects of the Global Financial Crisis.[2] However despite the strength of leading local retail banks in the preceding years only 19% of Kenya's population of 35 million as of 2009 were banked.[3] As a result, mobile payments have enabled the unbanked and under banked majority onto the financial realm by attracting over 18 million mobile phone users in Kenya into having access to mobile payments, where fewer than 4 million people have bank accounts.[4] This rapid uptake of mobile payments has become unprecedented and thus mobile payments have become common place in Kenya for the past 6 years.[5] The infrastructure in which mobile payments is used, the ubiquity and convenience coupled with the growing willingness of consumers to use it (mobile payments), made its implementation a tangible reality in Kenya. Mobile payments have afforded the scale and efficiencies and the flexibility and contextual appropriateness of informal markets that other similar services were unable to.[6] It has done so by enabling 40% of the adult population register as users of mobile payments through their subscription for mobile services from the Mobile Network Operators (MNOs).[7] Consequently, there are over 96,000 agents[8] where users can deposit[9] and withdraw their electronically stored funds.[10] There has also been an increased amount of cash deposits and withdrawals estimated at over USD 400 million per month in person to person transfers.[11] Companies also use the mobile payments platform for bulk distribution of payments, such as dividends and disbursing of salaries. Utility companies, such as electricity and water companies, use the same platform to collect payments through its 'bill pay' [12] function. This has shown a drastic shift in the heavy dependence on currency and paper cheques as mobile payments are slowly replacing

2 The Global Financial Crises of 2007-2008, caused by the sub-prime mortgages peaked in 2006, caused the values of securities tied to U.S. real estate pricing to plummet, damaging financial institutions globally.

3 Kenya Bureau of Statistics <http://www.knbs.or.ke/E-Resources.php>accessed 3 September 2013.

4 Ibid

5 Mobile Payments through the introduction of M-Pesa by Safaricom have been commonplace since 2007.

6 Amrik Heyer and Ignacio Mas, 'Seeking Fertile Grounds for Mobile Money' <http://www.pymnts.com/journal-bak/lydian-payments-journal-2010/seeking-fertile-grounds-for-mobile-money-2/> (accessed 3 September, 2013).

7 For the use of the mobile payment service, users have to register with a Mobile Network Operator.

8 www.safaricom.co.ke Mobile payment agents are the retail outlets through which customers can cash in and out their stored value. Their role and status shall be discussed in this paper.

9 This although not legally defined as 'deposits', under the Banking Act (1969) this term is still used to mean the same thing which shows the complex legal nature in which mobile payments operate .

10 These stored funds are electronically stored values against what each consumer has 'deposited'. There is no generally accepted definition of an electronic stored–value product much less those stored in mobile phones. However, the term "stored–value" is often used to refer to payment methods in which a prepaid balance of funds, or "value," is recorded on a device held by the consumer; this balance is decreased, or debited, when the devise is presented for payment in this case the devise being , the mobile phone.

11 Pauline Vaughan, 'The Transformational Potential for M-Transactions: Moving the Debate Forward' (The Policy Paper Series Number July 2007) <http://www.vodafone.com/content/dam/vodafone/about/public_policy/policy_papers/public_policy_series_6.pdf > accessed 19 November 2011.

12 The 'Bill Pay' function of mobile payments allows users to pay for their utilities bills, this has provided the opportunity for companies to engage their customers and streamline the payment of bills.

more traditional payment methods. Efforts to create a unified body of law for payment systems have so far been unsuccessful in many developing countries. [13] In part, the failure is due to the assumption that the existing law works well for the traditional paper based check system, and that problems have been created only by the evolution of new technologies.[14] This exemplifies the debate that regulation lags behind innovation and the difficulties that regulators have in establishing frameworks that support innovative products in markets. Moreover, this approach is one that the Kenyan regulatory environment has taken, as there is currently no specific regulatory framework for mobile payments. As a result, consumer protection remains one of the primary concerns that mobile payments has brought.

13 James Rogers, 'The End of Negotiable Instruments: Bringing Payments Systems Law Out of the Past.' (OUP 2012)

14 Ibid at

The Mobile Payment Players

2.0 The Mobile Network Operator

A Mobile Network Operator (MNO) is the telecommunications company that provides and extends the wireless network messaging functionality to provide payment services that enable customers to remit funds to each other that can be settled through its own established agent network. Individual payment transactions occur entirely within the MNO and do not require the service user to have a bank account.

The funds in transit – paid in by the remitter but not yet withdrawn by the recipient – are in principle on deposit in a segregated account with one or more banks (trust account in Kenya), so are within the formal financial system. Since the service provider is only executing client payment instructions and is not performing the credit evaluation and risk management function of a bank, these services do not, according to the Banking Act ,[15] constitute "banking."[16] Therefore the MNOs do not require the level of regulatory oversight needed for deposits held in banks. The depository bank is then seen not to have any involvement in or responsibility for payments through the MNO system. The MNOs provide the infrastructure and communications service while providing agent oversight and quality control, although this paper questions this oversight and control.

15 The Banking Act 1969 s 2 (a)(1).

16 The Act describes 'banking' as the accepting from members of the public of money on deposit repayable on demand or at the expiry of a fixed period or after notice. It also describes it as the accepting from members of the public of money on current account and payment on and acceptance of cheques; and the employing of money held on deposit or on current account, or any part of the money, by lending, investment or in any other manner for the account and at the risk of the person so employing the money.

Kenya's best known MNO is Safaricom which, although provides telecommunication services, is also a *de facto* a mobile money issuer. There is currently no law or regulation in Kenya establishing Mobile Network Operator as a distinct type of institution therefore Safaricom began operating pursuant to a 'No Objection' letter agreement with the Central Bank of Kenya.[17] Safaricom issues stored value to its M-PESA customers, who are also customers of the mobile phone company, Safaricom. Mobile payments in Kenya are carried out through the use of MNOs and this is defined as a MNO-led mobile payment system as opposed to a bank-led. In the MNO-led payment model, the MNOs offer mobile payment services as a means to add value to their core communications services. This however presents legal challenges that this paper will highlight in part. For instance, customer funds are commonly held in a prepaid account by the MNO or a subsidiary. Although in some jurisdictions even if the MNO is the business owner (the entity which assumes the bulk of the financial risk and operational responsibility of offering the service), a partner bank formally holds the license. If the funds are post-paid, the MNO can be considered to be providing short-term credit or payment service to its customers, in the same way as some three-party payment card schemes.[18]

2.1 The Bank

In the mobile payment context, banks offer banking services via the mobile device. They hold the e-float on behalf of the MNOs and handle cross-border transactions while managing foreign exchange risk. In Kenya, retail payments are dominated by banks whose primary function is to gather deposits for deployment in loans and other permissible investments. Banks are best positioned to employ risk management programs that ensure regulatory compliance.

The banks' role in the mobile payment value chain is important as the mobile payment system in exchange for e-float is deposited in bank accounts held by the mobile network operator. In efforts to diversify their risk, MNOs hold such deposits in different banks. These accounts are regular current accounts where MNOs have no restrictions of access. In turn, the banks face no special reserve requirements with regard to the MNO's' deposits. Similarly, there are no explicit requirements for theMNO to give notice of their intention to withdraw "large" quantities of cash at a

17 This refers to the Letter issued to Safaricom by the Central Bank of Kenya Authorising its operations after a risk assessment was conducted in February 2007. <http://www.gsma.com/mobilefordevelopment/wp-content/uploads/2013/09/enablingmobilemoneytransfer92.pdf> accessed 12 January 2012. Also Bankable Frontier Associates LLC (2010), "Enabling Mobile Money Transfer – The Central Bank of Kenya's Treatment of M-PESA", Alliance for Financial Inclusion.

18 In this model, the issuer (having the relationship with the cardholder) and the acquirer (having the relationship with the merchant) is the same entity. This means that there is no need for any charges between the issuer and the acquirer. Since it is a franchise setup, there is only one franchisee in each market, which is the incentive in this model. There is no competition within the brand; rather the competition is with other brands.

given point in time, which shows that these trusts are treated as any other current account deposit in terms of regulatory policy by the Central Bank. This then shows the vulnerability that exists within the framework which mobile payments is currently operating under as there are no legal obligations between the MNOs and the banks and if there are any these obligations are one of the banks and account holders.

2.2 The Agent

Agents are nonbank entities such as retailers (either the MNO's own retail centre or another retailer such as a small store) that handle customer registration and liquidity needs for the mobile money users, on behalf of the MNOs. The primary role of an agent is to accept and disburse cash and in essence providing cash-in and cash-out services from the consumer's mobile device. In this role, the agents serve as branches for the mobile network operators and act as the point of sale for the customer relationship. As the liaison between the MNO and the consumer, the agent bears responsibility for account opening, customer due diligence, and Know-Your-Customer (KYC) program compliance. The most typical candidates for agents are the retail sales stores and airtime resellers because they tend to have sufficient liquidity to satisfy consumers' needs to deposit and withdraw cash. This network of local agents expands the mobile operator's reach to rural areas in order to achieve a higher level of penetration in unbanked markets where there is no physical bank presence, which has also been one of the main advantages to mobile payments essentially enabling a branchless payment system, outside the traditional bank-led business model. Agents typically provide liquidity with funding from other business activities including selling airtime in addition to other merchandise. They receive commissions for transactions and hold balances on their own mobile phones. These mobile airtime balances and cash on premises are the critical elements of the agents' liquidity management system. Agents are also required to perform minimal customer due diligence which this paper will challenge as this due diligence is only limited to the provision of a postal address which this paper posits is not enough. Agents also report suspicious transactions in accordance with Anti-Money Laundering and Combating the Financing of Terrorist requirements as stipulated by the MNO they are attached to.[19] The agent is therefore the MNOs, interface between the cash flow and the consumer. To facilitate purchases and sales of e-float, mobile network operators maintain and operate an extensive network of over 96,000 agents across Kenya.[20] Registered mobile payment users can make deposits and withdrawals of cash (i.e., make purchases and sales of e-float) with the agents who receive a commission on a sliding scale for both deposits and

19 Agent Requirements for example are detailed in Safaricom's website, http://www.safaricom.co.ke/personal/m-pesa/m-pesa-agents accessed 24th October 2013.

20 < http://whiteafrican.com/wp-content/uploads/2013/09/MMU-Infographic-The-Kenyan-journey-to-digital-financial-inclusion.pdf> Accessed 24th October 2013.

withdrawals.[21] The agents hold e float balances on their own mobile devices, purchased either from the mobile network operator or from customers, and maintain cash on their premises. Agents therefore face a non-trivial inventory management problem, having to predict the time profile of net e-float needs, while maintaining the security of their operations. Their function is to provide cash in cash out transactions which cannot be executed without sufficient reserves of both mobile money and cash at the agent outlets. Mobile money liquidity and cash liquidity are therefore key areas of concern in a mobile money deployment.

Various models exist, through which agent networks operate. MNOs have evolved into having two tier structures with master agents who manage liquidity as the liaison between themselves and the individual stores, or sub-agents under their management framework. The master agent buys and sells cash from the MNO, makes it available to the sub-agents, and distributes agent commissions.[22] A final and more recent model allows a bank branch, referred to as a "super-agent," to perform the functions of the aggregator of the second model. The super-agent model is one example of the integration of mobile network operator services into the banking system. Other developments in this vein have seen users with accounts at certain commercial banks, being able to transfer funds between those accounts and their mobile payment accounts.

21 Id. ("Registration and deposits are free and most other transactions are priced based on a tiered structure to allow even the poorest users to be able to use the system at a reasonable cost. Transaction values are typically small, ranging from USD 5 to USD 30."); Mas & Radcliffe, supra note 5, at 170 ("[Retail] stores are paid a fee by Safaricom each time they exchange [cash for M-PESA credit] on behalf of customers.").

22 Bangens, Lennart, and Bjorn Soderberg. 2008. "Mobile Banking—Financial Services for the Unbanked?" SPIDER, The Swedish Program for Information and Communication Technology in Developing Regions. http://www.spidercenter.org/files/m-banking_study.pdf. accessed 14th June 2012

2.3 The Consumer

The 'consumer' in this paper is the mobile payment user. The mobile payment users have created a specific demand for mobile payments in Kenya. Their adoption and trust in the system has been one of the characteristics of mobile payments success. This is evident from previous payment instruments that were introduced to the market without an expressed demand from the consumers. It has been noted that the market environment in Africa and other developing countries is generally not consumer-oriented[23] Research on consumer protection and dissatisfaction for less sophisticated consumer segments in developing countries is sparse.[24] It is even sparser in mobile payments and retail banking service issues.[25]

23 Lyman, Timothy, Gautam Ivatury, and Stefan Staschen. 2006. "Use of Agents in Branchless Banking for the Poor; Rewards, Risks, and Regulation." Focus Note 38. Washington, D.C.: CGAP. <http://dev.cgap. org/p/site/c/template.rc/1.9.2585/> accessed 16 June 2011.

24 Ibid.

25 Brix, Laura, and Katharine McKee. 2009. "Consumer Protection Regulation in Low-Access Environments: Opportunities to Promote Responsible Finance." Focus Note 60. Washington, D.C.: CGAP. <http:// www.cgap.org/p/site/c/template.rc/1.9.42343/> accessed 21 June 2013

The justification for consumer protection regulation is at the onset to maintain consumer confidence in the financial system, to assure that a supplier on whom consumers rely does not fail. It is also to assure that consumers receive sufficient information to make "good" decisions and are dealt with fairly, consumer protection also assures fair pricing of financial services, and protects consumers from fraud and misrepresentation, and finally prevents discrimination against individuals.

2.4 The Background

The creation of a unified body of law for payment systems has so far been unsuccessful in most developing countries.[26] In part, the failure is due to the assumption that the existing law works well for the traditional paper based check system, and that problems have been created only by the evolution of new technologies.[27] Therefore in dealing with the disparate areas of mobile commerce law, one is constantly reminded of the tortoise and the hare, [28] as technology develops at an extremely fast pace. As a result, the formulation of new government regulations or legal principles governing new technologies practically always lags behind. Most governments act reactively and amend or create regulations after industry acceptance of these technologies has taken place. This eventually gives rise to the increasing and steadily widening gap between new technologies and adequate government regulation. The existing body of law is, however not entirely helpless and often times is able to adapt and tackle some of the emerging legal issues that mobile payments present. This is has been done through the process of drawing from precedents or the transplantation[29] of regulatory regimes from other jurisdiction and applying them to Kenya's.[30] There is, unfortunately and perhaps understandably, a limit to the ability of the law to adapt itself to emerging technologies: timely legislative intervention to supplant the existing law and to fill in the existing lacunae is often needed to ensure that the law remains current and relevant.[31] Therefore, the growth in mobile payments in recent years has raised concerns that existing legal and regulatory regimes are inconsistent or inadequate to deal with the issues mobile payments raise. This has in turn, caused some concern that application of too much traditional regulation will stifle growth. Consequently, it has been argued that modern information markets should largely be defined by agreements and other forms of market choice rather than by public regulation.[32]

26 James Rogers, 'The End Of Negotiable Instruments: Bringing Payments Systems Law Out Of The Past.' (OUP 2012).

27 Ibid.

28 Electronic Commerce Law country report at (2000) 27 Asia Business law Review 38.

29 The term 'legal transplant' is used to indicate the moving of a rule or a system of law from one country to another (A. Watson, Legal Transplants: An Approach to Comparative Law, Edinburgh, 1974).

30 Ibid.

31 The Diffusion of E-Commerce in Developing Economies: A Resource Based Approach by Zeinab Karake- Shalhoub, Lubna Al Qasimi. 2006.

32 Raymond T. Nimmer, 'International Information Transactions: an Essay on Law in an Information Society' 26 Brooklyn Journal of International Law 5(2000).

Consumer protection presents one of many legal and regulatory issues surrounding mobile payments in Kenya. Consumer protection can contribute to improved efficiency, transparency, competition, and access to retail financial markets. [33] Consumer protection is of particular importance in Kenya where financial education levels are generally lower and information flows constrained.[34] Since mobile payments provide one of the largest mass-market service provisions (as of May 2013 there are now 10.5 million active mobile payment users in Kenya[35]) the best strategy is to strengthen financial consumer protection. The financial sector regulators' responsibilty for oversight of financial services, particularly the Central Bank of Kenya and the Ministry of Finance have adequate authority to improve financial consumer protection through incremental improvements in the current regulation. The Central Bank of Kenya has been watchful and has also provided oversight and deliberate guidance from the very beginning.[36] However, this oversight and guidance has not been as exhaustive and extensive as it ought to be. While the CBK and Safaricom have addressed emerging challenges in the introduction of mobile payments however, the consumer protection measures that exist are not yet not codified in law.

Low-income consumers have been more vulnerable to the misconduct of providers and less able to protect themselves leading to loss of their income. MNOs therefore have a responsibility to inform their customers, and in turn customers have a responsibility to inform themselves.[37] However, this can be difficult for low-income customers due to limited awareness, knowledge, and skills to assess products' appropriateness, costs and risks. This means that policymakers and regulators should ensure that consumer protection measures adequately meet the needs of the poor or inexperienced consumers. Protection of consumers in any market has been emphasised as an important justification for government regulation of financial products. Firstly consumer protection increases consumer confidence in any financial system, which in turn reduces risks to financial stability. Consumer protection is needed to build trust in the financial system and, thus, to broaden and diversify the deposit base of banks. This in turn reduces the liquidity risk of the

33 Alliance for Financial Inclusion (2010), "The 2010 AFI Survey Report on Financial Inclusion Policy in Developing Countries.

34 A situation in which one party in a transaction, has more or superior information compared to another. In this situation Safaricom or any other MNO is considered to have more information than its consumers due to it not being a public entity but a private company with its strict non-disclosure practices.

35 Annual Report From Safaricom. www.safaricom.co.ke.

36 Bankable Frontier Associates LLC (2010), "Enabling Mobile Money Transfer – The Central Bank of Kenya's Treatment of M-PESA", Alliance for Financial Inclusion.

37 This would be similar to the Caveat Emptor Principle, where the purchaser assumes the risk that the product might be either defective or unsuitable to his or her needs. This rule is not designed to shield sellers who engage in Fraud or bad faith dealing by making false or misleading representations about the quality or condition of a particular product. It merely summarizes the concept that a purchaser must examine, judge, and test a product considered for purchase themselves.

banking sector. Better informed consumers also help foster financial stability by protecting themselves from incurring large exposure to market risk. This increases the transparency of credit risk assumed by the financial system and lowers monitoring costs for financial supervisors.[38] Secondly consumer protection, addresses the imbalance of power information and resources between consumers and their financial service providers, which highlights a typical market failure. Financial institutions know their services well but individual consumers may find it difficult or costly to obtain information on the financial products they purchase. In addition, complex financial products may be difficult to assess even when all the information is disclosed. Thirdly they promote efficiency and transparency of retail financial markets. Consumers who are empowered with information and basic rights are an important source of market discipline. This encourages financial institutions to compete by offering better products and services, rather than by taking advantage of poorly informed consumers.[39]

38 Chandra, Shalini; Srivastava, Shirish C.; and Theng, Yin-Leng (2010) "Evaluating the Role of Trust in Consumer Adoption of Mobile Payment Systems: An Empirical Analysis, "Communications of the Association for Information Systems Vol. 27, Article 29. Available at: <http://aisel.aisnet.org/cais/vol27/iss1/29> .accessed June 2013.

39 S R Weatherill and others, Consumer Protection Law (Ashgate Publishing Company 2005).

The Current Regulatory Framework for Consumer Protection

In the following section, I will review the current consumer protection regulation in Kenya, which has grown largely in response to expanded use of financial products. I will aim to show the fragmentation of the current regime and the gaps that it presents as a result of its fragmentation making an argument for at best, consolidation of the legislative instruments for consumer protection of financial services.

This is because the regulatory responsibility is divided amongst many bodies; this has engendered calls for rationalization and centralization as in many jurisdictions.[40] At the statutory level, Kenya has adopted electronic transactions legislation.[41] However, this is not considered sufficient for the needs of all commercial operators, including the needs of mobile payments providers.[42] In 2011, Kenya adopted the National Payment System Bill, which mostly contains regulatory content, but explicitly allows the use of electronic means when providing payment services.[43] The liability of the mobile network operator is limited in several ways, including, for losses arising from "particular circumstances," even if known to the operator.[44] The mobile network operator is also not liable for technical malfunctions resulting "from circumstances beyond reasonable control."[45] Consequently

40 A discussion on the consolidation of the regulatory regime for financial services has been brought forth in various discourses in Kenya, however at present none has been successful.

41 The Kenya Communications (Electronic Transactions) Regulations, 2009, 'The Electronic Funds Transfer Bill 2009'.

42 This will be discussed in the proceeding sections.

43 Ibid at its Article 2, sub-definition of "payment service provider."

44 Customer Terms & Conditions, SAFARICOM (on file with author) [hereinafter SAFARICOM Customer Terms & Conditions]; Terms & Conditions, VODACOM available at <http://www.vodacom.co.tz/vodacom-m-pesa/terms--> conditions (July 20, 2012) [hereinafter VODACOM Terms & Conditions].

45 Ibid.

useful elements for the assessment may be found in the contractual provisions of two major mobile network operators offering payment services.[46] Since the consumer protection regime for payment systems in Kenya is fragmented, similar transactions attract different levels of protection. Additionally, similar disputes are subject to resolution by different schemes. This paper argues that there should be an effort to rationalise the existing structure.

Before the implementation of the Consumer Protection Act 2012, consumer protection in Kenya lacked a cohesive policy and regulatory framework. The Banking Act gives authority to the Central Bank of Kenya (CBK) to regulate banking activities, but does not define the specific mandate for consumer protection beyond regulating in the interest of consumers.[47] The Banking Regulations of 2006[48] prescribe procedures to be followed for increasing the rate of banking and other fees. Particular rules govern unlawful, misleading and comparative advertising, and recourse mechanisms are left to individual banks. In practice there exist mechanisms of disclosure of prices and conditions of different financial services.[49] Because mobile payments have been successful under an undefined regulatory space, there has been no specific regulation about MNOs offering mobile financial services. However, the National Payment System Department (NPSD) of the CBK has provided oversight to mobile payments on the integrity of the on the integrity of information technology and the service delivery systems protecting customers from operational failures. The Restrictive Trade Practices, Monopolies and Price Control Act of 1989 is the most comprehensive legislation related to competition in Kenya. Although the act does not empower consumer advocacy organizations to lodge a complaint or contain provisions on consumer welfare, the Public Complaints Commission does provide third-party recourse for consumers of public sector services.

In December 2012, Parliament passed the Consumer Protection Act 2012 (the "Act") into law. Prior to the enactment of the Act, Kenya did not have a specific law that governs consumer protection. The Act provided a timely introduction into consumer protection in Kenya. However, the Act does not provide consumer protection for financial products and services. The new Kenyan constitution,[50] provided for the enactment of the Draft Consumer Protection Bill as there had been urgency in finalizing them. This shows the regulatory capacity of Kenya to legislate. The need for customer protection called for a legislation that would strengthen protection for users of regulated providers while also offering

46 Customer Terms & Conditions, SAFARICOM [hereinafter SAFARICOM Customer Terms & Conditions]; Terms & Conditions, VODACOM available at http://www.vodacom.co.tz/vodacom-m-pesa/terms--conditions (July 20, 2012) [hereinafter VODACOM Terms & Conditions].

47 The Banking Act and Banking Regulations of 2006 have implications for consumer protection in Kenya as they regulate the limits on interest recovered on defaulted loans and the misleading advertisement for deposits. They also prohibit the charging of fees on savings and fixed deposit accounts, requiring approval by the Minister of Finance if a bank wishes to increase its rate of banking.

48 Banking Act and Banking (Increase of Rate of Banking and Other Charges) Regulations of 2006 (consumer protection-related) (amended through 2010)

49 Ibid.

50 Kenya Constitution Promulgated on the 27th of August 2010 necessitated various Bills to be enacted.

protections to users of unregulated providers such as MNOs. Kenya already has essential pieces of payments laws in place which have not adequately protected consumers primarily because they did not apply to all types of non-cash payments.[51] The use of these new technological platforms does not fit neatly into the legal categories used by existing consumer protection statutes. The Kenya Information and Communications Consumer Protection Regulations[52] outline the rights and responsibilities of consumers and contains specific provisions that define the obligations of service providers related to complaint handling, information disclosure, billing practices and data privacy.[53] The rules also require service providers to submit for approval a commercial code of practice that defines the service provider's policies and procedures related to compliance with the provision. However because the National Payment Bill is formally established in law, the Central Bank of Kenya and the MNOs have worked under the understanding that the regulatory structure of the industry will be clarified in future.[54] At the same time, consumers have already adapted the mobile payment service to uses that exceed the current regulatory definition of the MNOs channel. These uses include storing their value for a short time in their mobile phone account in the same way a current account would be used.[55] Moreover, other supporting service providers in the value chain[56] are building and deploying new services based on the mobile money platform such as M-KESHO and M-KOPO.[57] All of these new mobile money services and products are developments that show the innovation and dynamism of the industry which has extended the reach of financial services to the unbanked. The particular risks that affect consumers are varied; system problems,[58] performance issues and even company failures are some of the problems with negative implications for consumers, unless the regulatory framework keeps pace with the rapid evolution of the industry.

The Kenyan consumer is therefore left to figure out what protections apply to each competing new payments system. This new integration of mobile telecommunications companies and the financial industry provides Kenya with an opportunity to

51 Electronic and mobile payments are all forms of Non- Cash Payments.

52 The Kenya Information and Communications Consumer Protection Regulations <http://www.cck.go.ke/links/public_notices/2011/Adherance.pdf.> accessed14th September 2013

53 Ibid.

54 This was through a 'No Objection Letter' Issued by the then Minister of Finance, the Late Hon John Michuki, who gave Safaricom the 'go ahead' to continue its operations with very little oversight from the Central Bank.

55 This is like a virtual account, in which users store their money for a short period before making payments.

56 This phrase is used to mean the mobile money ecosystem.

57 This is a banking service by both Equity and Safaricom where money can earn interest from as little as Ksh1 through the transfer of one's funds from their Equity Bank Account to their M-Pesa account and also make deposits through their M-Pesa account to their M-Kesho account. Other features of the account include Micro-credit facilities (emergency credit availed through M-PESA), Micro-insurance facilities as well as a personal accident cover that translates into a full cover after 1 year. To open this account, one must be an M-PESA subscriber.

58 Operational Risks pertaining to the technology used.

harmonise [59] and extend consumer protections for mobile payments. However two things should occur immediately: Firstly, as MNOs regulator, the Communication Commission of Kenya (CCK) should publicly commit to include in its mandate the need for consumer protection. Secondly, MNOs should include in their contracts the full consumer rights provided under existing law. Thirdly, the Central Bank of Kenya, through its supervisory and oversight role, should ensure that it does what it can under existing statutory authority to ensure that existing consumer protections are applied to new payment methods. Kenya should have a reform legislation that would provide authority for the Consumer Protection Act to have mandate over financial services and products.

Therefore, Kenya's inherent problem is that there is a lack of coherence in consumer protection and market oversight. The split in responsibility has made it difficult for regulators to take a strategic view of priorities across the entire retail financial services sector. Decisions are driven by different legal duties and powers of individual regulators such as the Communications Commission of Kenya and the Central Bank of Kenya. Having two regulatory regimes for what is often from the consumer's perspective a single product or service can result in different rights and a divergence in protection for personal and small business consumers. Mobile payment users may not fully understand which regulations apply to a payment transaction and how these may differ depending on the payment method and platform used, the parties involved in the payment transaction, and the nature of the product purchased.

The lack of understanding stems from the fact that the different bodies (banks, MNOs and agents) whose operations are often overseen by different regulatory bodies also operate under different sets of regulations. Consumers are therefore unclear over what redress rights they have which entity to turn to if there is a payment-related problem. Awareness making it pertinent for organisations and regulators to emphasise customer protection especially with the new type of customer being reached innovatively. The CCK has been willing to license MNOs to carry out mobile financial services as long as they list the service in their license agreement. This poses regulatory difficulties because the CCK does not have authority over financial services and if MNOs list mobile payments as a service they provide then it creates regulatory inconsistencies resulting from traditional separation.[60] This is because the Commission's mandate is limited to licensing all systems and services in the communications industry, including telecommunications, postal/courier and broadcasting. The Commission also manages the country's spectrum and numbering resources and facilitating the development of e-commerce. The Commission also protects consumer rights within

59 Harmonization here refers to the need for a consolidation of legislation due to the fragmentation that existed before The Consumer Protection Act.

60 This notion shall be discussed in the paper.

the communications environment.[61] The Commission manages competition in the sector to ensure a level playing ground for all players,[62] regulating retail and wholesale tariffs for communications services, and managing the Universal Access Fund (USF).[63] The Commission also monitors the activities of licensees to enforce compliance with the licence terms and conditions as well as the law.

In 2008, the CCK created a Consumer Affairs Division[64] and by 2010, the CCK issued the Kenya Information and Communications Consumer Protection Regulations.[65] The regulations outline the rights and responsibilities of consumers and contain specific provisions that define the obligations of service providers related to complaint handling, information disclosure, billing practices, data privacy, and other issues. The rules also require service providers to submit for approval a commercial code of practice that defines the service provider's policies and procedures related to compliance with the provisions. The regulations are recent and untested but they do represent the most comprehensive set of consumer protection regulations issued by a regulator in Kenya.

Therefore the current state of consumer protection regulation presents a distinction between its state and practice. As mentioned, neither the regulations nor the authority to regulate the sector are formally established in law. The CBK and the MNOs have worked under the understanding that the regulatory structure of the industry will be clarified in the future, with the expected passage of the National Payments Bill and subsequent regulation. It is with this lack of formality in the current regulatory framework that has implications for consumers which regulatory body to appeal to if a problem cannot be resolved with a merchant. This is especially so since consumers have already adapted mobile payments service to uses that exceed the current regulatory definition of the MNOs channel such as storing their value for a short time, similar to the way a bank customer would use a current account. Moreover, other supporting service

61 These rights however are limited to the functions of telecommunications and not of the financial services.

62 The players here refer to the various Mobile Network Operators.

63 The Kenya Communications (Amendment) Act, 2009, provides for the establishment of a Universal Service Fund (USF), administered and managed by CCK. The purpose of the Fund is to support widespread access to ICT services, promote capacity building and innovations in ICT services in the country.

64 This Division

65 The Kenya Information and Communication Act (1998) Chapter 411A. <http://www.cck.go.ke/regulations/downloads/Kenya-Information-Communications-Act-Final.pdf>

providers in the mobile payment system are building and deploying new services based on the mobile payments platform.[66] Banks, for example, are linking bank accounts with the mobile accounts, some even enabling providers to link subscribers' funds to their bank accounts.

66 Examples include KOPOKOPO LTD a service that provides low cost software service for mobile money repayment mechanism for Small and Medium sized Enterprises.

The Challenges for Regulators

A common justification for the regulation of financial services is the need to protect the consumer. Economic and social explanations and justifications for regulation both focus in part on the consumer as the principal beneficiary of regulation. Consumers, however, are a heterogeneous rather than a homogeneous group. Some are affluent, others are not. Some are highly educated, others are not.

Protecting such a wide and diverse group presents the authorities with a range of challenges. One challenge is to design policies which take appropriate account of the interests of those consumers who might be described as disadvantaged.[67] The convergence,[68] of telecommunications and finance has given rise to regulatory challenges for regulators. This section explores several reasons why convergence has become problematic for regulators. The limited regulatory intervention in these hybrid business models has been left to market forces with only minimal general product regulation such as consumer safety. In marked contrast, both telecommunications and financial firms have been subjected to significant sector specific regulations.[69] The ownership of MNOs is restricted to multinational corporations, such as Vodafone, or Airtel who have to invest heavily in getting their services to serve the Kenyan population and on the other hand, banks have to raise the minimum capital requirements.

67 Peter Cartwright, ' The Vulnerable Consumer of Financial Services: Law, Policy and Regulation', T Wilhelmsson "The Informed Consumer v the Vulnerable Consumer in European Unfair Commercial Practices Law – A Comment" in G Howells, a Nordhausen, D Parry and C Twigg-Flesner (eds) Yearbook of Consumer Law 2007 (Ashgate, 2007) 211 at p 213.

68 Convergence here shall be used to mean the hybridised business model where two sector specific industries are merged to provide a service.

69 The difference in the regulation of banks and Central Bank of Kenya and MNOs and the Telecommunication, the convergence.

The beginning of this convergence raises questions about the regulatory regime the industry will face. The split in responsibility makes it difficult for regulators to take a strategic view of priorities across the entire retail financial services sector. Decisions are driven by different legal duties and powers of individual regulators. The existing laws do not provide a sufficient legal setting for the mobile payment sphere. This paper highlights some of the challenges that regulators will face when establishing a consumer protection regulation in a jurisdiction that does not have consolidated consumer protection legislation such as Kenya.

4.1 Different Objectives for Regulation Of The Sectors

Telecommunications have been provided by monopolies for years until the liberation and privatization of telecommunications companies that oligopolies developed.[70] The telecoms industry in Kenya, just like the rest of the world, is going through profound changes. In the past decade, technological advancement and regulatory restructuring have transformed the industry. Markets that were formerly distinct, discrete and vertical have coalesced across their old boundaries with a massive investment of capital - much of it originating from private sector participants. The result is new markets, new players, and new challenges. Market liberalisation efforts have also picked up ensuing the successful partial privatisation of Telkom Kenya Ltd[71] divestment of government of Kenya's 25% stake in Safaricom Ltd through a public listing[72] and the launch of fourth mobile operator Econet Wireless Kenya.[73] This has resulted into some of the world's best known telecommunication providers – Vodafone, France Telecoms and Essar Communications through their investments in Safaricom Limited, Telkom Kenya Limited and Econet Limited respectively - being major players in the Kenyan market. Furthermore there is on-going infrastructural developments by operators have largely been focused on network expansion for increased nationwide coverage.

Therefore the Kenyan government has found little reason to regulate quality or prices in this highly competitive telecommunications sector. The main objective of regulating MNOs is to ensure that consumers are protected from operators reducing output to increase prices on low quality services.[74] The other objective should be to ensure that the new population included in the mobile payments ecosystem are protected. A third objective would be for financial institutions to ensure that the money pooled in the mobile money ecosystem does not cause systemic risks in the long run. The convergence of these industries makes regulation more difficult as there is a need to determine which objectives to pursue and how to accomplish them now that several industries provide multiple services.

70 Raymond U. Akwule, 'Telecommunications in Kenya: Development and Policy Issues' Telecommunications Policy, Volume 16, Issue 7, September–October 1992, Pages 603–611.

71 This happened in December 2007 http://www.telkom.co.ke/index.php?option=com_content&view=article&id=60&Itemid=95Accessed 12 September 2013.

72 This listing was done in May 2008.

73 This was done in November 2008.

74 Blackman, C. (1998). Convergence Between Telecommunications And Other Media: How Should Regulation Adapt? Telecommunications Policy, 22:3, 163-170.

4.2 Inconsistencies In Regulation Resulting From Traditional Separation

As this paper has attempted to show, a regulatory vacuum is created due to the interconnectedness of telecommunications and finance. When none of the existing government agencies has issued regulations on the new services, the regulations could fall under the jurisdiction of two or more agencies which leads to jurisdictional conflicts. MNOs are supervised by the CCK. While retail payments provided by banks are regulated by the CBK. In trying to resolve this examples from other juridictions may be illustrative. In the UK, wired television was under the jurisdiction of Oftel[75] while the Independent Television Commission (ITC) regulated wireless television. When a service such as British Interactive Broadcasting emerged conflicts arose,[76] this type of problem eventually led to the creation of the converged regulator Ofcom.[77]

4.3 Regulatory Arbitrage

When there are multiple regulators, companies can select the ones that advance their interest the most. This could mean they select, for example, the most lenient regulator or take advantage of the rules that most benefit them. This is problematic when regulation does not yet exist for emerging convergent services that could fall under the supervision of more than one regulator. In the presence of these alternatives they can choose the one that would entail the least regulation, which may not necessarily be the best option for society or the industry as a whole. It could be argued that multiple regulators are desirable because they can foster institutional learning by eliminating obsolete legal models and expanding desirable ones. This argument, although theoretically feasible, may not be practically possible. This is because the interests of companies are not aligned with those of the government. Companies want to maximize profits while governments aim to maximize societal welfare. The rules that companies may wish to have applied to them do not necessarily lead to benefits for society

4.4 Uncertainty

A great challenge for regulators is their inability to reliably forecast the future due to rapidly changing technology, which has given rise to unforeseen new products and services. Without knowing how technology is going to evolve, regulators can only issue rules for the problems faced today, but it is always possible that these rules will cause problems when new technologies become available. This is what mobile payments have brought forth – the fact that mobile devices have 'leap-frogged' the

75 The Office of Telecommunications (Oftel) (the telecommunications regulator) was a department in the United Kingdom government, under civil service control, charged with promoting competition and maintaining the interests of consumers in the UK telecommunications market. It was set up under the Telecommunications Act 1984 after privatisation of the nationalised operator BT.

76 Collins, R., 'Back To the Future: Digital Television and Convergence In The United Kingdom.' Telecommunications Policy, (1998). 22:4-5, 383-96.

77 Ibid, The Office of Communications), commonly known as Ofcom, is the government-approved regulatory and competition authority for the broadcasting, telecommunications and postal industries of the United Kingdom.

advancement of retail payments where it is possible to make remittances and payments in a manner similar to check payments and other pre-existing payment systems, created great concern at least initially for banks who felt that a new competitor had entered the market . The regulator then has to decide whether to do nothing or to intervene. The limited capabilities of the previous retail payments such as MoneyGram[78] and Western Union[79] options saw that the same service could be offered at a much cheaper cost. In light of this continuous innovation, regulators need to find regulatory frameworks that allow them to better cope with uncertainty.

78 See, MoneyGram https://www.moneygram.com/wps/portal/moneygramonline/home/sendmoney?CC=GB&LC=en-GB&gclid=ClvplZr037oCFYbLtAodwIAA1Q Accessed 12th of September 2013.

79 Western Union < http://www.westernunion.co.uk/> Accessed 12th September 2013.

Rationale for Consumer Protection for Mobile Payment Users

This part of the paper will discuss the rationale for consumer protection, which at its apex addresses disparities in consumer- supplier relationship. It will examine various justifications for consumer protection of financial services and products and then elaborate the risks that mobile payment users are exposed to as a result of an unregulated mobile payment system. It will also form the crux of this paper.

This paper has identified who 'the consumer' is and who are concerned with their protection. This paper has also shown the relationship between consumer protection and the market economy. In the legal literature, consumer protection is generally explained, and justified, by the concept of the "weaker party." Consumers are considered to be "weaker" than their contracting partners and the professionals, and are assumed to be unable to protect their interests due to inferior bargaining power.[80] The concept of vulnerability asserts that some consumers are more vulnerable than others, an aspect that has been recognised by legislation. We know that vulnerable consumers exist, even if we may disagree about how to identify them, and about how their interests might best be addressed.[81] Focusing on the exercise

80 Hugh Beale, Inequality of Bargaining Power, 6 OXFORD J. LEGAL STUD. 123 (1986) (U.K.); JOHN KENNETH GALBRAITH, THE NEW INDUSTRIAL STATE 213– 20 (1971); Friedrich Kessler, Contracts Of Adhesion: Some Thoughts about Freedom Of Contact, 43 COLUM. L. REV. 629, 632, 640– 41 (1943); Spencer N. Thal, The Inequality Of Bargaining Power Doctrine: The Problem Of Defining Contractual Unfairness, 8 OXFORD J. LEGAL STUD.

81 Peter Cartwright, 'The Vulnerable Consumer Of Financial Services: Law Policy And Regulation.' and T Wilhelmsson "The Informed Consumer v the Vulnerable Consumer in European Unfair Commercial Practices Law – A Comment" in G Howells, a Nordhausen, D Parry and C Twigg-Flesner (eds) Yearbook of Consumer Law 2007 (Ashgate, 2007) 211 at p

of market power, exploitation theory argues that consumers are in need of protection for two reasons: First, consumers have few options but to purchase and contract on the terms set by increasingly large and powerful companies.[82] Second, companies are able to exploit significant information and sophistication disparities in their favour.[83] However, exploitation theory has not prevailed, and economists no longer regard the theory as an explanation or justification for consumer protection.[84] The reason for this is that exploitation theory fails to take into account competition between companies and the fact that any bargaining power that companies have visa-vis consumers is limited through competition from other companies.[85] Therefore, insofar as consumers are today deemed in need of protection from an economic perspective, it is not because they are considered "weaker" and at risk of exploitation by large companies. Rather, it is because consumers know less about products and contracts than professionals do.[86] It is sometimes argued that the state, through the law, should play only a restricted role in protecting consumers, because consumer protection is most efficiently achieved by the operation of free and open markets. The law should be used to ensure that the markets function as freely as possible. Where markets do not work perfectly, the law should intervene to address this failure, provided this can be done cost effectively. While accepting the importance of market and social goals, it is argued that the distinction between the two is not clearly drawn, and that some approaches could be viewed under either heading.[87]

Consumer protection presents one of the many legal and regulatory challenges that surround mobile payments in Kenya. Consumer protection can reduce information asymmetries and ensure that the interests of end-users of financial services are protected.[88] It can contribute to improved efficiency, transparency, competition, and access to retail financial markets.[89] Consumer protection is of particular importance in Kenya where financial education levels are generally lower and information flows constrained. Since mobile payments provide one of the largest mass-market services (as of May 2013 there are now 10.5 million active mobile payment users in Kenya), the best strategy for strengthening financial consumer protection in Kenya, as in any country, would be

213.

82 Ibid at 85.

83 Giesela Ruhl, 'Consumer Protection in Choice of Law,' 44 CORNELL INT'L L.J. 569 (2011)

84 Haupt, Schaffer, Alan Schwartz, 'Legal Implications of Imperfect Information in Consumer Market's, 151 J. INSTITUTIONAL & THEORETICAL ECON. [JITE] 31, 35– 36 (1995) (F.R.G.); Fernando Gomez Pomar & Nuna Garupa, Max Weber Lecture: The Economic Approach to European Consumer Protection Law (Nov. 21, 2007).

85 Ibid, at 560.

86 Ibid

87 Ibid at 88

88 Information Asymmetry creates an imbalance of power in transactions which can sometimes cause a market failure resulting from moral hazard, and information monopoly. Most commonly, information asymmetries are studied in the context of principal–agent problems. John O. Ledyard "market failure," The New Palgrave Dictionary of Economics, 2nd Ed (2008).

89 Ibid.

grounded in pragmatic solutions to problems that affect the large number of consumers.

The financial Retail payments raise the additional issue of consumer protection. Independent from the kind of commercial relationship between the service provider and the user of the service, either durable or occasional, rules on transparency and protection of customers must be implemented. In addition to regulatory policy focusing on the structure of the market and its infrastructure, the mobile payment instruments require adequate protection of users. In particular, in addition to transparency requirements, know-your-customer (KYC) guidelines, and observance of Anti Money Laundering (AML) regulation, the protection of users' funds and their traceability are a must, as well as protection from any risk arising from the use of electronic means and the intermediation of non-financial agents. Indeed, once service providers are duly regulated under a risk-based approach and a playing field is ensured in the market to guarantee competition and competitiveness, all other needs for protection can be addressed under a general understanding of consumer protection and an adequate consideration of the role of agents.[90] Regulators in Kenya however have largely adopted a watch and learn regulatory approach regarding the electronic money industry and non-banks providing these services.

90 B. Bossone and M. Cirasino, "The Oversight of the Payment Systems: A Framework for the Development and Governance of Payment Systems in Emerging Economies", July 2001, The World Bank and CEMLA.

Consumer protection essentially entails: Protecting the consumer from fraud or exploitation by providers with significant market power, ensure minimum disclosure and quality standards for clients, support confidence in the financial system. Conducting of business rules, competition policy, ombudsman schemes minimum disclosure and contracting standards, consumer education surveillance and enforcement measures. The consumer's inability to judge the safety of their funds and the need to ensure that operators have proper incentives to respect contracts and consumer interests justifies a need for regulation in this context. However, instruments of consumer protection can sometimes limit service and product innovations. Standardisation can enhance transparency, the capacity for consumers to compare offers and enforce minimum levels of quality, and ensure that contingency arrangements are in place in case of a technical failure of the mobile payment service.

5.1 Protection of Consumer Funds

Due to their wide customer base, MNOs are well placed to reach customers with affordable financial services. The MNO's existing customer base, marketing capabilities, physical distribution and infrastructure and experience with high volume low value transaction makes this possible. Despite these advantages, there has been blurred lines between what constitutes taking deposits as from the public – even for purposes of effecting payment rather than for saving – and accepting public deposits in the conventional sense a an activity almost always reserved for prudentially regulated financial institutions such as commercial banks. These funds are held in a bank which is subject to strict prudential requirements and supervision.[91] The protection of consumer funds is therefore usually a priority for any financial regulator. The loss of funds imposes distrust in the system and as loss of funds can have serious consequences for customers, as well as for public confidence in financial systems. Banks are usually required to comply with prudential rules created to ensure systemic stability and depositor protection and are also covered by deposit insurance in many jurisdictions.[92] In addition, governments may provide an implicit guarantee to bank depositors, especially when banks are systemically important.[93] In mobile payments MNOs collect funds in exchange for electronically stored value, without being subject to the full range of prudential rules imposed on banks. Also, there may be models where even if client funds sit in a bank account, they receive a different regulatory treatment than those applicable to bank deposits. Funds collected by Safaricom for M-Pesa, which customers increasingly use as a short-term savings mechanism, are deposited in pooled trust accounts at several commercial banks, for the benefit of the customers. In the event of insolvency however, there is no mechanism in place for customers to claim trust assets. This therefore leaves the consumer with no recourse if the said bank becomes insolvent. This further highlights the complexity that these electronically stored value poses. The definition of these 'deposits' needs to be clarified in the mobile payment system, because as liquid assets are most often required to be maintained as accounts with a prudentially regulated bank, they may be maintained as other "safe assets," such as government securities, although such securities may not always be as liquid as bank accounts.[94] This brings forth regulatory challenges in that client assets are left unsecured due to the lack of regulatory framework. It is therefore difficult to assess whether they should be subject to a safety net or some deposit insurance scheme.[95] This paper posits that they should be covered by a deposit insurance scheme, where the government would implicitly guarantee the protection of these funds in accordance with the current regulatory structure despite the fact that they are legally not responsible.

Protecting consumer funds are measures aimed at ensuring funds are available to meet customer demands for cashing out electronic value. Such measures typically include restrictions on the use of such funds, requirements that such funds be placed in their entirety in bank accounts or government debt and that there should be a diversification of floats

91 The term Bank as used in this paper refers to any supervised and prudentially regulated financial services institution that is commonly, but not always a bank.

92 Consumer Protection Diagnostic Study: Kenya, Financial Sector Deepening. January 2011.

93 Ibid.

94 Safe Assets, 'deposit' provide challenges in the regulation of mobile payments because of their legal ambiguity definitions and their ambiguity.

95 This assessment would somewhat be after a proper definition of what the electronically stored value is and what banks would consider it to be thus making it easier to offer the same protection as they would other legally defined 'deposits'

across several financial institutions.[96] A key prudential requirement typically imposed by regulators to ensure a customer's money is available when the customer wants to redeem it is that the MNO, maintains liquid assets equal in value to the amount of money issued electronically. One common approach is to require assets to be isolated and held in a bank account. Kenya's regulators have ensured that the funds are deposited in one or several commercial banks that are fully prudentially regulated so that all monies in the account are safeguarded.[97] These requirements may be seen as stringent than those imposed on deposit taking financial institutions, "which are typically subject to reserve requirements mandating only some small portion of overall deposits to be kept in liquid form – typically cash – to satisfy potential depositor claims."[98] Customer funds are usually pooled and held by the bank(s) in the name of the issuer. Regulation should require that the funds backing the mobile money stored value are protected from institutional risks, such as claims made by creditors in cases of issuer bankruptcy. This protection is guaranteed by establishing a "trust" or fiduciary agreement, under which funds are held on behalf of the clients. The concept of a trust originally was developed in common law jurisdictions, but recently some countries with a civil law legal tradition have adopted similar concepts. France, for example, passed a law establishing the concept of "la fid`1ucie" in 2007, [99] and this concept is referenced in the Central Bank of Congo's e-money regulation as a mechanism to ensure that customers can recover their funds in the event of issuer failure.[100]

If Safaricom for example, was to become insolvent, these failings could lead to complications and delay in distribution and placed consumer funds at risk of set-off and consequential diminution. This is because while Safaricom is not seen to be a monopoly but rather as having multiple dominant positions.[101] The threat of large depositor losses has to be met through having means of depositor protection inplace. Furthermore, mobile financial services providers particularly if they operate on a global scale (perhaps by liaising with an international financial group) may become so large and interconnected over the years

96 Tarazi, Michael and Paul Breloff, July 2010, "Nonbank E-Money Issuers: Regulatory Approaches to Protecting Customer Funds." Focus Note 63. <http://www.cgap.org/gm/ document-1.9.45715/FN_63_Rev.pdf> accessed on the 13 September 2013.

97 Slightly different approaches have been taken by regulators that, rather than requiring the entire e-money float to be held in a bank, have allowed it to be invested in low-risk securities such as government bonds.

98 Michael Tarazi and Paul Breloff (2010), "Nonbank E-Money] Issuers: Regulatory Approaches to Protecting Customer Funds," CGAP Focus Note 63. Available at <http://www.cgap.org/sites/default/ files/CGAP-Focus-Note-NonbankE-Money-Issuers-RegulatoryApproaches-to-ProtectingCustomer-Funds-Jul-2010.pdf>Accessed 13 August 2013.

99 http://www.legifrance.gouv.fr/ <affichTexte.do?cidTexte=JORFTEXT000000821047&dateTexte=>.

100 Banque Centrale du Congo, Instruction n.24/2011.

101 Market dominance, which is a stricter concept than market power, is typically defined by two conditions, a relatively high market share, which Safaricom has and significant barrier to entry into the relevant markets occupied by the dominant firm. The first condition holds in all markets where Safaricom is active. The second may hold in the agent market but not in the mobile telephony market due to the Communications commission of Kenya's action.

that their failure could cause disruptions within the wider financial markets. This threat is perhaps even more distinct with respect to conventional providers of banking services as the channels of risk distribution may be less visible in the mobile money value chain compared to financial institutions with physical branches and subsidiaries. This consideration reveals how essential it is to clearly define the scope of mobile payment services in the larger context of the financial industry. More importantly mobile payments has turned into a 'shadow' banking system,[102] undermining government supervision and the rather comprehensive regulation of traditional banking. Regulation should ensure that in protecting consumer funds MNOs should maintain liquid assets equivalent to the total value of the customer funds collected.[103]

The protection of consumer assets should go beyond issues of fraud and misuse to include protection of consumer's deposits savings and other similar financial assets in the event of a bank collapse. No system is in place for customers to claim trust assets. The MNOs approach to the stored value or customer funds created or presumption that the MNO was the legal owner of the funds and uncertainty as to the beneficial owner of the monies. This introduces a risk to client that in the event of insolvency, the deposit banks might consider mobile network operators rather than the individual consumer to be the owner of the 'deposits'. The Kenya Deposit Protection Fund only protects deposits in current accounts savings accounts and time fixed deposit accounts. However funds held in trust are treated as distinct from individually owned accounts and therefore insured separately.

Caps are sometimes placed on interest rates, restrictions on product cross-subsidisation, and pricing policies may be regulated. These kinds of measures can be useful in certain circumstances. But when applied to other market environments for which they were not conceived, they can easily inhibit innovations made possible by mobile entry. Operators and regulators together need to review limitations that may pose unnecessary constraints. Incomplete contracting standards can also be a problem for the development of new service models. For example, agents may be required to validate the authenticity of documents or signatures. The protection of consumer funds is therefore usually a priority for any financial regulator. The loss of funds imposes distrust in the system and as loss of funds can have serious consequences for customers, as well as for public confidence in financial systems.

The loss of funds usually occurs either due to illiquidity or insolvency of the MNO or the bank where the funds are held. Mobile payment users may have problems withdrawing their funds due to their agent being illiquid, or if their transaction does not go through due to technical difficulties either through a lack

102 This phrase has been used severally in various literatures to define the parallel, informal banking system that mobile payments have afforded.

103 That is the total value of electronic value issued and outstanding, also known as the "e-float".

of connection or a system outage. Customers may also lose funds through fraudulent agents, or if they charge unexpected or unauthorized fees, fees which may not always be clearly disclosed to the customers. If the customers, personal information (Personal Identification Numbers) are stolen, wrongfully accessed, shared, or used to conduct unauthorized transactions or for commercial purposes.

MNOs collect funds in exchange for electronically stored value, without being subject to the full range of prudential rules imposed on banks. Also, there may be models where even if client funds are held in a bank account, they receive a different regulatory treatment than those applicable to bank deposits. In the event of insolvency however there is no mechanism in place for customers to claim trust assets. This therefore leaves the consumer with no recourse when and if the said bank becomes insolvent. This further highlights the complexity that these electronically stored value poses, as they are not considered bank deposits, it is therefore difficult to assess whether they should be subject to a safety net or some deposit protection scheme. This presents the same complexities that the administrators found in the Lehman Brothers case,[104] where the Supreme Court was unable to determine with any certainty either the amount of client monies held by Lehman Brothers International Europe (LBIE) to be pooled, or, once determined, who was entitled to participate in or receive money from that pool. A factor in this uncertainty was, no doubt, the fact that, as one of the largest investment banks operating in the United Kingdom prior to its collapse, LBIE undertook multiple complex financial transactions on a daily basis.

The case for complementary measures to be put in place to ensure that, the funds are protected is compelling. Regulation can target protecting consumer funds through not only requiring providers to keep the equivalent of the outstanding electronic value issued in a bank account, but also limiting investment of the funds to low-risk, highly liquid assets and prohibiting the use of the funds for purposes other than withdrawals and transfers according to customer requests. Regulators should also maintain that the trust holders maintain liquid assets equivalent to the total value of the customer funds collected (i.e., the total value of electronic value issued and outstanding, also known as the "e-float"). Although this, as earlier observed, is a more stringent requirement than imposed on deposit-taking financial institutions, which are typically subject to reserve requirements, this treatment reflects a fundamental difference among banks, MNOs and their respective business models. A bank's business is predicated on the ability to intermediate capital, which is taking money from those who have it and provide it (in loans or other products) to those who need it. Nonbanks, on the other hand, are expressly prevented from

104 Lehman Brothers International (Europe) In Administration) and In The Matter of Insolvency Act 1986 [2012[UKSC 6 .

intermediating deposits and thus must make money in other ways, such as transaction charges, lowered airtime distribution costs, and reduced customer input. Liquid assets are most often required to be maintained as accounts with a prudentially regulated bank but sometimes they may be maintained as other "safe assets," such as government securities, although such securities may not always be as liquid as bank accounts.[105] In Kenya, where applicable regulation is currently being drafted, Safaricom maintains fund liquidity by placing collected cash in prudentially regulated banks pursuant to a prior agreement with the Central Bank of Kenya.

The ownership of the funds has also come under much scrutiny. There are expectations for there to be a requirement that accounts where funds are deposited are individual accounts in the name of the customers or pooled trust accounts to the benefit of the customers. Futher, providers should be prohibited from pledging the funds as collateral. They should also offer legal protection against other creditors in the case of insolvency of the issuer or the bank where the funds are deposited. The EU E-Money Directive (2009), for instance, requires contracts to state clearly and prominently the conditions of redemption, including any fees, and limits charges on redemption to a few specific circumstances. A policy recommendation for this safeguard would be through having a 'deposit' protection scheme or a stored value protection scheme as it would be called.

Deposit protection schemes play an important role in protecting consumers by providing compensation should a firm find itself unable to meet its obligations to them.[106] It can be argued that consumer protection was the main motivation behind the creation of original deposit protection scheme. The benefits and technical feasibility of extending deposit insurance to mobile money have been clearly demonstrated in the United States, where, as long as e-float is placed in an insured depository institution, it is considered an insured deposit. For pooled custodial accounts, there is pass-through protection for each customer up to the insurance limit. Deposit protection through insurance might be a viable solution, but before such a system is set up, it is essential to assess who will fund it, how the premiums will be determined and assessed, and what impact these premiums will have on the fees charged to customers for mobile money services. However, as discussed, to the extent that the underlying customer funds are kept in bank accounts, such funds are exposed to the risk of bank failure. Even in circumstances where deposit insurance exists, the value of pooled accounts is often much higher than the applicable deposit insurance coverage limits. As electronic value offerings grow in volume and popularity, and as evidence mounts that e-money

105 In West African countries under the jurisdiction of the Banque Centrale des Etats de L'Afrique d'Ouest (BCEAO), regulation also permits funds to be invested in securities issued by registered companies.

106 Payment, Clearing And Settlement Systems In The CPSS Countrieshttp://www.bis.org/publ/cpss105.pdf accessed on the 20th of October 2013

schemes are increasingly being used as savings vehicles,[107] regulators may want to consider extending deposit insurance protection at the level of individual customer e-money balances or alternatively raise the ceiling for pooled accounts.[108] Many developed countries already provide such deposit protection. The United States, for example, expressly characterizes the funds underlying stored-value cards as "deposits" covered by deposit insurance as long as such funds are placed in an insured institution.[109]

A key prudential requirement typically imposed by regulators to ensure a customer's money is available when the customer wants to redeem it is that the non-bank mobile money provider maintains liquid assets equal in value to the amount of money issued electronically.

Consumer funds in the mobile payment system are pooled and held by the bank by the Mobile Network Operator. Regulators should require these funds are protected from institutional risks, such as claims made by creditors in cases of the MNO's bankruptcy. This protection is guaranteed by establishing the "trust" or fiduciary agreement, under which funds are held on behalf of the customers as previously discussed. [110] This is similar to the Lehman Brother's problem regarding mixing of client and own funds which resulted in new client asset rules. MNOs in Kenya currently use this mechanism, which in the Central Bank of Congo's e-money regulation is meant to ensure that the mobile payment user can recover their funds in the event of the MNO's failure.[111] The risk of mobile money customers losing the money they have stored in the system is mitigated if the non-bank mobile money provider does not intermediate the funds;[112] and customer funds are isolated from the Mobile Network Operator's funds and protected from claims by their creditors. Certain risks posed by licensed non-bank mobile money providers can been successfully mitigated through prudential requirements that

107 In the Philippines, an estimated 10% of unbanked users save an average of US$31 (one-quarter of their family savings) in the form of e-money (Pickens 2009). In addition, nearly a third of banked customers in Kibera, Kenya, keep a balance in their M-PESA account, and a fifth of the unbanked interviewees in Kibera use M-PESA as a substitute for informal methods of savings, especially keeping money at home. See Morawczynski and Pickens (2009).

108 On the other hand, deposit insurance is usually funded by premiums paid by participating financial institutions, which typically pass these costs along to their customers. Thus, inclusion of e-money issuers in a deposit insurance system may make their services slightly more expensive.

109 The Federal Deposit Insurance Corporation (FDIC) is a United States government corporation operating as an independent agency created by the Banking Act of 1933. Prudential requirements aim to maintain the integrity of the institution's capital and a certain level of liquidity. They are intended to mitigate credit and liquidity risks and might include minimum capital ratios, capital adequacy measurement systems, reserve requirements, or other measures intended to preserve the liquidity of the provider.

110 The 'Trust' here is the trust account.

111 Banque Centrale du Congo, Instruction n.24/2011. <http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000821047&dateTexte=.>

112 Financial intermediation is business conducted or services offered by a financial intermediary (typically a bank, but a non-bank financial institution) that accepts money from individuals or entities with capital surpluses and then lends it (directly through loans or indirectly through capital markets) to individuals or entities with capital deficits to earn a profit. Several risks can be associated with financial intermediation, such as interest rate risk, market risk, credit risk, off-balance-sheet risk, foreign exchange risk, country or sovereign risk, technology risk, operational risk, liquidity risk, and insolvency risk.

safeguard funds entering the system and meet customer demand to cash out electronic value.

5.1.1 The Legal Status of Agents

This part of the paper discusses the legal status of agents and suggests that due to the fact that there is no legal accountability for agents, customers are not protected. They provide the network through which mobile payments are executed and, as mentioned earlier, are the bridges to cash and channels for financial inclusion. Since mobile payments almost solely rely on agents for its customer interface, it is necessary to ensure that providers comply with applicable regulations when using third parties just as if the services were rendered directly by the providers. The private sector sometimes interprets specific wording of legal texts and research as implying more than retaining the provider's liability for regulatory compliance, that is, to encompass legal liability for any and all acts of their agents. This is not necessarily desirable from a business and policy perspective. Legal liability for agents simply means limiting opportunities for providers to circumvent applicable regulations, including conduct-of-business rules. This provides one of the complexities that regulators have in establishing an appropriate framework and consumers when seeking redress, because, agents have a service level agreement between them and their providing MNOs.[113] This agreement however does not create an agent–principal relationship in the true legal sense. The provider should respond to consumer claims even if the agent acts fraudulently (e.g., it should not avoid regulation and evade responsibility in a case where the agent accesses client bank information and withdraws money from the client's account). Obviously the provider can seek redress against the agent, but the customer should be able to file a complaint with the provider, who should be responsible for ensuring data privacy and security.

Failure to hold providers liable for agent compliance may hinder regulators' ability to achieve the policy objectives discussed in this paper, as implementing rules for protecting customers when third parties are involved in service delivery becomes challenging in practice. It essentially shifts the burden for monitoring agents from the supervised entity to the supervisor (with significant added supervisory costs) and to consumers (with significant added social costs, especially when dealing with low income customers).[114] Thus, providers' liability for the acts of their agents is a fundamental principle for outsourcing in financial services.[115] With a specific focus on the agents' actions related to delivery of mobile payments, ensuring that mobile network providers are liable does not create unlimited liability and should not create unreasonable burdens on providers. As in other types of outsourcing, regulators should expect to see effective risk management systems in place and timely and appropriate actions by providers (including

113 Safaricom Ltd has one with M-Pesa agents.

114 Denise Dias, Kate McKee, 'Protecting Branchless Banking Consumers' <http://www.cgap.org/publications/protecting-branchless-banking-consumers> accessed 9th August 2012

115 Ibid.

redress for consumers) when problems with agents are detected. Ensuring provider liability by regulation (and indeed, implementing other measures discussed in this paper) does not require making new business models proposed by nonfinancial firms wait until a complete regulatory framework is developed. Discussion over whether to hold off on market conduct rules such as including establishing explicit provider liability for agent acts until mobile payments have developed have been going on. However, the policy recommendations here are that, the regulator should take actions towards mobile network providers that will prevent problems, by setting minimum business practice standards such as the provider's liability for agents' compliance with regulation if liability over agents should not be extended towards them. It should also give legal tools for regulators and consumers to solve problems when they arise and create a level playing field that fosters competition and healthy market development.

Some jurisdictions such as the Reserve Bank of India, Malaysia, Indonesia, and the Philippines, have created rules for e-money issued by non-banks and have focused on specific regulation for agents who process mobile money, which have addressed a previous regulatory vacuum.[116] In Mexico, a 2008 regulation gave clear powers to the banking supervisor for the first time over agency schemes set up by banks, allowing direct inspection of agents if necessary.

116 BIS Papers No 62 Financial Sector Regulation For Growth, Equity And Stability. Proceedings of a conference organised by the BIS and CAFRAL in Mumbai, 15–16 November 2011 Monetary and Economic Department January 2012.

Kenya's experience, in contrast, has been the lack of clarity as to the legal authority that regulates mobile payments. This overlapping or unclear authority can create opportunities for undesirable business practices and reduce effectiveness of supervision as providers may question supervisor's actions.[117] When more than one regulatory body is involved, coordination and cooperation is important, particularly for mobile payments.

5.1.2 Redress Mechanism

Most MNOs provide customer service through their agents, and through their telephone help lines. These channels however are often seen as cumbersome for most mobile payment users and are not effective in dealing with the difficulties often experienced by mobile payment users.[118] Available recourse mechanisms may not be effective, convenient, widely publicized, or affordable and customer problems that can be exacerbated when the customer interface is done exclusively by third-party agents and customers are less educated and experienced in the use of formal financial services. In February 2009, Safaricom reported fielding 17,000 calls per day on the M-PESA

117 The Communications Commission Of Kenya, For Example, Recently Issued Substantial Consumer Protection Regulations With Implications For Mobile Payment Services (Kenya Gazette, 23 April 2010).

118 The FSD 2008 M-PESA survey reported that 75% of users did not know how to access customer service. Yet in the FSD/CGAP 2010 FGDs, participants were ubiquitously clear how to resolve problems ("You call customer care") as well as conveying a clear sense of how long it will take for the problem to be resolved ("72 hours"). Moreover, the same survey showed that 92% of problems are resolved within a day.

help line.[119] More recent data reflects even more frequent use of the customer care line. However, MNOs do not publicize the recourse options for lodging complaints against their agents with the same clarity or ubiquity as the pricing structure or customer service channels. For example, Safaricom claims to intervene on customers' behalf in complaints against agents; nevertheless because their relationship with their agents is not a legal one there are only liable to a certain point and not when there are instances of agent fraud or loss of funds. Furthermore, and depending on the funding source used by your mobile payment service, consumers do not have strong protections over disputes on fraudulent payments or unauthorized charges. This poses an increasing risk to consumers who rely on mobile payments and therefore forms a basis for review. There should therefore be a minimum requirement for establishing recourse mechanisms, one that makes consumers aware of the procedures for reporting and their complaints follow up should be codified and that MNOs in the market operate these procedures in a standardised way. While Kenya has statutes protecting consumers from unauthorized credit card and debit card transactions, similar statutes do not however exist for stored valued payments such as mobile payments. Some MNOs offer protections on their own, which are outlined in customer agreements. However, these protections can be rescinded or modified by the provider at any time.

There is little doubt that the creation of mechanisms for alternative dispute resolution such as ombudsmen have contributed considerably towards obviating some of the barriers to consumers' access to justice. A policy objective here is to make consumers have access to recourse directly or through public enforcement with public bodies such as the government. The limitations of redress through the private law, and in particular the existence of transaction costs, have demonstrated the necessity for their mechanisms for consumer redress. The CCK[120] should ensure that it develops regulations that compel all companies to have complaints procedures to keep customers satisfied and to address their problems. The CCK should in fact ensure that such channels for complaints are clearly specified and communicated to customers, including procedures for escalation, specifying the regulator as the referee of last resort for resolving only those individual cases that cannot be settled with the operator concerned. The reporting of operator complaints to CCK should help identify issues that need addressing more generally. The CCK should engage in publication of complaints information as a way to keep operators focused on customer service even when providers are compliant with consumer related regulations and offer out-of-court complaint and redress procedures. In the countries studied, a common channel to lodge complaints is the telephone, but call centres seem to present many challenges and can be particularly burdensome for low-income customers. Holding providers liable for complying with applicable regulations when they use agents is an important step

119 Lyman, Timothy, Mark Pickens and David Porteous. (2008). Regulating Transformational Branchless Banking: Mobile Phones and Other Technology to Increase Access to Finance. Focus Note 43. Washington DC: CGAP

120 Communications Commission of Kenya (CCK).

for ensuring adequate redress but it is not sufficient. Regulations can set minimum standards for internal dispute resolution channels and procedures, and some standards will need to be tailored to mobile payments. In achieving adequate redress mechanisms for mobile payment users, regulators should be cognizant of significantly less experienced and resourceful customers. This has been the case with bringing the unbanked into the financial realm and in order to keep these new consumers satisfied and financially included, businesses must provide suitable education about the service, the rights of the consumers to seek redress and how to go about obtaining it directly from them, or from elsewhere, if still not resolved by them.

5.1.3 Privacy and Data Protection

Privacy and data protection concerns are distinct issues that arise in any electronic platform especially payment systems. Due to the convergence of the industries, consumer protection policies are not specific to the needs of mobile payments. In this case privacy is of great concern although not one that the Kenyan market has highlighted. However, despite this fact, regulators have been confronted with the question of how to regulate in such a manner that balances consumer rights to privacy with the objectives of law enforcement officials who wish to combat money laundering. Transactions and personal data are transmitted through mobile phone networks, handled more often by third parties such as agents, and accessed remotely by customers and financial institution employees, the risk of inappropriate access and usage rises. Besides the technological aspect, consumers' lack of education and lack of experience with formal financial services and technology may raise data security risks.

The main concern has been over the users Identification, geographic location and the value of their transaction. Kenya's current legislation does not define who can get access to a mobile money trail and how, when or under what conditions such access may be obtained. This complicates efforts to keep consumer information private while at the same time conflicts with the desire for regulators to keep customer funds safe against financial crimes. In addition, the privacy regulations that apply to banks in respect of customer financial records do not extend to Mobile Network Operators. While MNOs report having instituted internal controls to minimize unauthorized access to consumer information, consumers simply have to trust the MNO to ensure that these are observed. In this context, simple and transparent mechanisms are needed through which users can authorize an entity to access this kind of information. Proper data protection laws need to integrate mobile money data or other information emanating from money transfers and ensure that such data are not used for undesirable activities in the framework of general legislation on data retention and privacy. Currently, the licensing requirements for communication services mandate MNOs to provide access to user phone records in response to a legal court order, but this does not explicitly cover mobile money records. As a result, who can access an individual's mobile money records, when and for what purpose is not clear. Kenya's Draft Regulation for the Provision of Electronic Retail Transfers attempts to address the issue of privacy by mandating a provider to maintain confidentiality of all consumer information, stating that, "A provider is allowed to share any consumer information only with the consumers or their authorised agent (authorized in writing), the Central Bank, in the public interest or in response to formal legal requests."

A brief examination of data privacy and bank secrecy regulations in developing countries reveals a patchwork of rules issued by a variety of agencies with overlapping jurisdiction and oversight. In India, for instance providers are liable for the acts of omission and commission of their agents in all respects, including bank secrecy, while Kenya currently has no rules for agents of mobile payments providers. Design and enforcement of data privacy and security rules require some level of coordination between supervisory and regulatory authorities, as mobile payments cuts across different sectors such as banking and telecommunications. Regulations should be consistent and robust enough to hold providers responsible for data privacy, and they should be liable for privacy breaches and misuse of customer data. Regulation also needs to be technology neutral, since imposition of specific standards and protocols in a rapidly evolving industry is likely to hinder innovation. Specific requirements should be imposed only to correct identified problems in existing businesses.

There is a trade-off between enhancing data security and keeping the costs down to allow profitability of low-value financial transactions. The low-end market may require technologies that are somewhat less safe than others, based on availability (e.g., security features that can be implemented in less expensive mobile phones) and customer user-friendliness (e.g., interfaces that are most appropriate for low income customers). Also, data privacy concerns may pose barriers to cross-border data transmission, inhibiting the ability of providers to offer faster and more reliable remittance services through electronic channels. In most situations, providers and regulators will be able to agree on technological platforms and business models that align each other's goals, but this requires an open dialogue between them, particularly when there are major current regulatory obstacles to overcome.

In any case, regulation will not eliminate security and privacy risks. Supervisors should evaluate the provider's risk management and mitigation systems and its procedures to handle cases of privacy and security breach. In cases such as Kenya, the regulator has engaged closely with the providers to help identify system and in-built technology solutions to observe and potential consumer problems. Supervisors should also be satisfied with the terms of outsourcing and partnership agreements to make sure such terms do not impact responsiveness to consumer claims related to data privacy and security, including when agents are involved. 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. Mobile money providers have internal controls to minimise unauthorised 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. MNOs have developed various systems to protect customer privacy. Typically MNOs back up their IT systems (at least) daily, and the USSD[121] and the STK[122] channels used to transact mobile money customer orders have so far proven to be sufficiently secure. USSD is also session-based, which leaves no traces of the transaction once the session is closed. SMS is encrypted over the SS7 links. Customers are also responsible for protecting their password, PIN number, and other sensitive information.

Consumer education can help to reduce breaches of privacy, and most mobile money providers take initiative to build customer awareness and capacity to prevent fraud by employees or third parties. The regulator could design and enforce a wide array of privacy-related requirements and require local hosting and specific procedures for back-ups and physical site security. However, compliance costs should be properly assessed and solutions discussed with mobile money providers, which seem particularly committed to addressing security risks and challenges. Data security is a big concern for consumers, as almost half of those who've never made a mobile payment cite this as their reason why. Mobile payments are making progress here, and according to the report, have stronger data security than traditional point of sale systems. Mobile payment technology permits end-to-end encryption, while under the traditional payment system; financial data often is stored or transmitted in an unencrypted form at some point during the payment process.[123]

5.1.4 Fraudulent, Misleading and Deceptive Commercial Practices.

The laws of Kenya ensure that user of credit cards or prepaid debit cards are protected if their cards are stolen or misused.[124] However, due to the fragmentation of the current regulatory regime, these laws do not apply to all new types of payment systems including mobile payments.[125] If the transactions are processed and settled through an existing credit card network, and appear on the credit card bill, then consumers are

121 Unstructured Supplementary Services Data (USSD)

122 SIM Application Toolkit

123 Protecting Branchless Banking Consumers: Policy Objectives < http://www.pymnts.com/journal-bak/201/protecting-branchless-banking-consumers-policy-objectives-and-regulatory-options> accessed June 2013.

124 Ibid

125 Ibid at 151.

entitled to all available protections. If the transaction amount is deducted from the consumer's deposit account with a financial institution, it should receive the same protections as any other electronic fund transfer. If the transaction is funded by a debit against a prepaid card, the protections for unauthorized use may be missing, and there will be no legal guarantee of a protection in the event of a dispute with a merchant. However, mobile payments are different in that the payment service is provided directly by the MNO and the charges appear on the customer's mobile payment statement, and therefore escaping the consumer protections entirely afforded to other forms of payments systems. Levels of fraud have become common and M-PESA reports that it handles about 50 cases a month of fraud, most of which are customers defrauding customers. M-PESA also deals with agents defrauding customers and claims to have recourse channels. For its part, the National Payment System Department (NPSD) claims to monitor fraud incident reports.[126] Neither entity publishes reports on this activity so all information about the recourse channels is gathered from interviews with M-PESA and NPSD staff.[127]

5.1.5 The Disclosure of Information To Consumers

Mobile payments can exacerbate information asymmetry when it involves multiple entities that charge separate fees for their services making it challenging for customers to deduce the final cost of the services they have used. Appropriate disclosure from all these entities should be expected by consumers.[128] The OECD report on Consumer Protection in Online and Mobile Payments identifies the need for clarity,[129] transparency and completeness in information disclosure. Clarifying the rules before the infrastructure for new services is fully created should reduce the cost of complying, since the protections can be built into the new products instead of being added later. Assuring consumers through regulation that they are protected if something goes wrong will allow their choice of payment service to be guided by underlying considerations of price, service and convenience, regardless of whether they choose an existing provider or a new entrant. Clarity and certainty will be good for consumers and for competitors. Permitting variations below baseline consumer protections will just confuse customers and hurt the entire market.

M-PESA's experience with pricing disclosure reveals some of the complexities of consumer protection measures in this area. M-PESA has one of the most transparent pricing schedules of any financial service provider in Kenya. The company expends significant effort to ensure that customers have

126 The National Payment System Department, Central Bank of Kenya <www.centralbank.go.ke>.

127 Ibid

128 Report on Consumer Protection in Online and Mobile Payments (OECD Digital Economy Papers No. 204) (Aug. 17, 2012

129 Clarity here is used to denote the need for the regulation to be explicit and clear in its meaning, to avoid misinterpretation.

access to consistent pricing information at the time of inscription and at every agent's place of business. Safaricom for instance has a readily observable track record of publishing its tariffs and supporting multiple, third-party customer surveys. There is however room for improvement for other MNOs to follow suit in that, due to the fact that there is a clear financial literacy concern documented in other pieces of literature. The field work also suggested that M-PESA agents explain that most customers only make transactions in the lower two tariff tiers and therefore don't pay attention to other parts of the tariff structure. Some agents also explain that many subscribers simply avoid some of the M-PESA services, such as mobile top up, for example, because they don't want to bother with something that looks complicated to them. Financial services and terms tend to be inherently complex.

A FinAccess study found that many consumers are challenged in fully understanding financial concepts and characteristics of formal financial services: only about 37% of respondents could correctly solve basic numeracy problems.[130] It is not easy to make pricing understandable to mass market consumers. This information asymmetry can lead to market failure through the low value, high volume payments made out over the mass market service that mobile payments provide. Tariff structures will be easiest for agents to explain and customers to understand if basic conventions are used across all providers. Safaricom and other MNOs have already set a very solid benchmark for industry practice and this could be translated into regulation in a way that is flexible but that guarantees a minimum level of tariff transparency.

Agents can also—deliberately or accidentally—fail to disclose prices fully or charge unauthorized fees. Countries have taken different approaches to these issues. Brazil and Mexico prescribe specific rules for price transparency at agents (e.g. agents should post signage with fees), whereas in India and Peru, such standards are set in general consumer protection regulations. In India and Brazil agents are prohibited from charging fees directly to customers, though banks may charge more for agent transactions—in comparison with branch transactions—so long as the customer is informed. Regulations should require contracts to be as short and simple in language as possible, and to include all fees and charges. This is done through signage posted at agents and printed marketing materials, as well as in transaction receipts that contain information about each transaction. This disclosure helps consumers identify the responsible entity when problems arise, thereby facilitating complaint filing. Regulators also should consider how providers communicate product features to their clients, especially in the case of electronic stored value services. Regulators should be aware of these differences when creating disclosure rules. Sometimes

130 Mark Flaming, Alexander Owino, Katharine McKee, Nicola Jentzsch, Simone di Castri, Bilha Maina, Moses Ochieng, Daryl Collins and Brendan Ahern. Consumer Protection Diagnostic Study Kenya (2011) http://www.fsdkenya.org/pdf_documents/11-02-22_Consumer_diagnostic_study.pdf accessed 20th June 2013.

providers go beyond the minimum standards in helping ensure that customers understand new services, for their own business reasons.

The Policy Recommendations

6.1 The Extension of Deposit Insurance

Deposit insurance is meant to protect bank customers from a bank's inability to pay its debts. Bank failures and the recent financial crisis have resulted in a rapid increase in the number of countries, currently and rising, that have a government or private mechanism for insuring bank deposits. [131]

The success of mobile payments has rested in part on the trust that consumers have in one of the market leaders in mobile payments, Safaricom. These include a large number of poor and developing countries. Deposit insurance is not just for the benefit of bank customers. Trust is an important element in any formal banking system and more so in the mobile payments system as more and more people are coming to rely on its platform. Since, mobile money or e-float is typically held in a bank,[132] regulators in Kenya do not extend deposit insurance to customers of e-money accounts issued by Mobile Network Operators. The custodial accounts holding the e-float do benefit from deposit insurance on the one hand , however, because the funds are pooled, insured amounts are typically well below the e-float total. The deposit insurance, designed for individual bank account holders, provides insurance on deposits up to a maximum of KSh 100,000 in Kenya, this insurance would do little to cover mobile payments e-float amount.[133] In

131 International Association of Deposit Insurers at< http://www.iadi. org/aboutiadi.aspx?id=79.>Accessed 7th September 2013.

132 Another safeguarding measure is private insurance. The European Union (EU), for example, permits safeguarding of funds backing e-money through insurance. EU Directive 2007/64/EC permits non-bank e-money issuers in lieu of liquidity provisions, to insure or comparably guarantee the funds backing e-float in an amount payable in the event that the non-bank issuer is unable to meet its financial obligations. EU Directive 2007/64/EC, Article 9.1(c) incorporated by reference from Article 7.1 of EU Directive 2009/110/EC (2009). It is not clear if any e-money issuer has availed itself of this private insurance option.

133 The trust responsible for the M-PESA e-float is charged 0.01% of deposited e-float as an insurance premium, though such expenses may be reimbursed from interest accruing on the e-float

addition, deposit insurance benefits the named holder of the account, which in cases where e-float is not held in trust, is often the e-money issuer. Extending the benefit of deposit insurance to e-money is, in principle, a relatively simple endeavour. However if the trust and faith in the banking system erodes, a run on mobile payments services could be sparked, thereby exacerbating the position of the banks in which it holds deposited funds. Thus mobile payments deposits are virtually completely uninsured against bank failure. Therefore, in protecting consumer funds, there should be a basic regulation with simple and clear rules to ensure appropriate liquidity and ownership of funds collected against the electronic value issued. Regulation can also set minimum standards for fund redemption to avoid undue restrictions including in the event of insolvency of the provider or the bank where the funds are deposited.

6.2 Ensuring Safety and Reliability of Services.

Operational risk in mobile payments systems is tantamount in the adoption of mobile payments as a national payment system. The over reliability of this service as the main platform for making payments and remittances across retail payments imposes great pressure on an adequate working system. Therefore, there should be an effective monitoring of emerging consumer issues and a decision on when and what type of regulatory action is necessary and effective to avoid loss of confidence or curve abuse by Mobile Network Operators. Regulation should require Mobile Network Operators to ensure reliability, availability and safety of services, without prescribing specific technology, systems and procedures. There should also be aware of threats that are outside the scope of financial authorities such as theft and laws on physical security requirements at agent's sites and the protection of mobile money against financial crimes such as money laundering and fraud.

6.3 Reducing Opportunities For Agent Fraud

The legal status and the liability of agents in mobile payments systems as discussed earlier in this paper, would ensure that mobile network operators ensure that their agents are compliant with the minimum standards set out for them by regulation. This can be done by ensuring that there are transaction limits set out for agents and that there is a set principles for agent selection and monitoring , without creating overly burdensome minim standards , such as minimum capital requirements for agents.[134] Regulation should be uniform across all providers to screen, qualify and monitor agents. The regulation implemented should review the providers' internal controls and processes to identify, measure, and mitigate these risks and ensure systems are in place to handle consumer complaints related to agent acts and assess whether initiatives to increase consumer awareness may have greater impact than regulation in some situations.

134 Currently MNOs require their agents to have a minimum of KSH200, 000 to be held at a bank before obtaining authority to act as an agent.

6.4 Ensuring Clear and Effective Disclosure

To balance the information asymmetry, as a justification for consumer protection, there should be an adequate and clear effective disclosure of information to consumers. These include the requirement of agents to post applicable fees, price disclosure, requiring contracts to be simple and include all relevant fees charged to be communicated to consumers.

6.5 Privacy and Data Protection.

The protection of privacy and consumer data in electronically stored money systems is an area that Kenya has not fully developed. Regulators should keep mobile network operators responsible for compliance with data privacy and bank secrecy regulations even when using agents or third parties. Existing rules applied in other payment systems should be applied and emerging models and evaluation should be assessed through the increase of interagency coordination for designing and enforcing these rules. Even though the assumption always made is that the cost of implementing security requirements and profitability in serving low income clients who have low value transactions is not considered proportionate. This can be mitigated by being flexible in considering models that aren't complex or rigid.

6.6 Ensuring that the Redress Mechanisms are Accessible and Effective.

The role of having an effective redress mechanism cannot be understated especially in mobile payments where the majority of the users are from low income backgrounds. Policies should be developed that would ensure that the existing rules for out of court redress and complaint channels apply to mobile payments or set specific standards tailored to new models as necessary. These mechanisms should be effective and should match existing transacting channels such as those for other payment systems such as the redress procedures and channels meeting minimum standards and the avenues are communicated clearly and consistently.

Conclusion

Consumer risks exist in mobile payments as in any other type of payment systems. There is no single regulatory approach to consumer protection that will work in all contexts, and none will eliminate all risks.

The current success that services such as M-Pesa has afforded the Kenyan economy has shown that although the benefits that this payment system has brought forth in an exceptionally short period, the risks to a stable financial system are imminent if careful oversight is overlooked. Despite the fact that mobile payments have reduced important shortcomings commonly associated with informal providers such as loss of customers' fund or other operational difficulties such as service discontinuity by the mobile network operator, there should be a balance that allows innovation that increases financial access and ensures a degree of consumer protection.

This paper has attempted to identify several priority policy objectives and regulatory measures that would guide consumer protection regulation in mobile payments. It has identified how several overarching policy objectives such as holding providers liable for compliance with applicable regulations when using agents and suggested the role that non regulatory measures, such as voluntary industry standards and practices, can play a role in protecting mobile payments customers it also proposes stronger consumer lobbying for a better consumer protection oversight. This paper hopes that the future regulation and supervision agenda should be informed in turn by analysis that quantifies and explores in more depth the behaviour and perceptions of mobile payments consumers, and the nature, incidence, and consequences of the problems they face in different forms. This is because consumers need to be convinced that mobile payments systems are both sufficiently trustworthy and economically worthwhile. Putting the consumer at the heart of the regulator's decision making maintains the focus on competition for delivering consumer benefits and helps to address areas where the market does not fully deliver. Therefore, consumer protection should go beyond handling consumer complaints. Having a consolidated legislature that has responsibility for consumer's protection and a framework that is fit for purpose in this environment would be ideal, although not a panacea would provide a useful starting point. Regulation here should not aim for an institutional change in its framing but to consider incremental changes that address the main risks aforementioned.

Regulation should aim to establish a culture of security that promotes trust in mobile payments, where effective enforcement of privacy and consumer protection. Due to the convergence and the interconnectedness of these two industries, the telecommunications and financial industries need to strengthen cross border cooperation that goes beyond licencing. But regulation in Kenya is hampered by the lack of resources and expertise which are common themes and difficulties with enforcement and encouragement of consumer protection measures. Customer interoperability,[135] that entails, cross-selling of services, product suitability, and deposit insurance in nonbank e-money issuing are some of the next generation consumer protection regulatory topics in mobile payments that require further research and experimentation. A modernised and consistent regulatory framework would enhance consumer protection; maintain the safety and soundness of the Kenyan payment system.

In conclusion, regulation and supervision are not sufficient to deal with all consumer protection problems. Sometimes problems are rooted in consumers' lack of understanding, knowledge, and awareness with regard to financial services and redress mechanisms. Well-targeted initiatives to improve financial literacy and increased awareness can play an important role in reducing risks for consumers and increasing effectiveness of regulatory action.[136] In order to ensure effective and proportionate financial consumer protection regimes it is important that all stakeholders participate in the process, from policy makers to financial institutions to consumer advocates and other civil society actors.[137]

135 The ability for mobile payment users to transfer money or payments across different Mobile Network Operators.

136 Protecting Branchless Banking Consumers: Policy Objectives , < http://www.pymnts.com/journal-bak/201/protecting-branchless-banking-consumers-policy-objectives-and-regulatory-options/> (accessed September 8, 2013).

137 Ibid.

Kenya Bankers Association
13th Floor, International House, Mama Ngina Street
P.O. Box 73100– 00200 NAIROBI
Telephone: 254 20 2221704/2217757/2224014/5
Cell: 0733 812770/0711 562910
Fax: 254 20 2221792
Email: consumerguide@kba.co.ke
Website: www.kba.co.ke

KENYA BANKERS
ASSOCIATION

One Industry. Transforming Kenya.