over the transaction history over its mobile money service. The borrower's mobile money account is associated with his or her phone number. Neither the credit scores nor the positive credit history that develops are available to credit reference bureaus and so other potential lenders lack such data to inform their lending decisions.

If the MNO mobile money service is dominant, lenders may face information asymmetries that reduce the quality of their credit evaluations and lending decisions. This may present barriers to entry, growth and innovation in mobile financial services, reducing competition and increasing costs of lending, and so borrowers' costs of borrowing. The relationship between credit eligibility and phone number may become another factor that raises switching costs not only in mobile credit but also in mobile telecommunication services.

The competitive advantage achieved through such innovation can be considerable. Where banks already have credit data on their customers, they can leverage such data for mobile lending to the same customers. However, lack of access to the extensive, current data and credit scores generated by the dominant mobile money transaction data may raise barriers to entry for alternative lenders, and switching costs for customers. This may result in limited competition, and could account for the high interest rates that these types of services, which are growing quickly, can offer. For example, KCB M-Pesa offers loans at 4 per cent per month, which is far higher than rates that can be obtained from the banks.

As the market develops, financial regulators will doubtlessly take an interest in the availability of data for lending decision-making, whether through credit bureau reporting or otherwise. One question will be whether the lenders should report not only negative credit histories but also positive credit histories to credit reference bureaus and whether this should be made available regularly enough to be 'real time.' Regulators may also take an interest in whether credit scores generated by algorithms using data held by MNOs that have dominance in the market (i.e., where they are the only ones that can generate such data) should somehow be made available to other banks.

Greater access to such data will allow a larger number of lenders to make better informed lending decisions, which should reduce the cost of credit and accelerate financial inclusion. Such competition should also enable the reduction in cost of credit to be passed through to consumers, resulting in lower interest rates on loans.

Again, of course, the regulator faces the dilemma of when, if at all, to intervene in the market. The kind of innovations being witnessed take not only investment, but more importantly sheer initiative, cleverness and drive, as well as capacity within the players involved. These features need to be encouraged, and the most obvious way is to allow them to reap rewards from their innovations.

At some stage, regulators are likely to consider requiring open access to data where it is an 'essential facility' for mobile credit when the provider is dominant. They may regard the data on a customer's transaction history as not merely something that the mobile money provider is entitled to use exclusively but actually something in which the customer himself or herself has an interest. In time, this may result in customers having a right to use such data not merely for services provided by a select number of partner banks, but with a broader range of potential lenders. Standards for how customers' transactional data is secured, accessed, analysed and shared (and who owns it) may be required to spur on development of mobile financial services.

3.7 Consumer protection

3.7.1 Transparency, disclosure and effective consent

The upsurge in mobile financial services raises a host of consumer protection issues. The services are new mass market products that are widely used and known. They are among the most exciting services to appear on the scene, and so have a high visibility.

Although there is demand for them, customers may lack knowledge of available alternatives and the general and financial literacy necessary to make well informed decisions. When customers face significant impediments or costs in their search for alternatives, or where there are only a small number of providers of the more convenient services (such as mobile credit), providers may be able to set prices and quality of service without regard to competition or consumer pressure.

Consumer protection and competition issues are closely interrelated. For example, transparent and simple pricing makes it easier to compare services. This creates competitive pressure for providers to improve price, quality, variety and innovation. Where there is competition, consumers may also have difficulty accessing and assessing information to compare the offers available in the market from different providers. For instance, many customers are confused about charges for transfers to other mobile wallets and payments to utilities, schools and merchants.[111]

Some of the weak protections for consumers have significant consequences. For example, some mobile money providers do not clearly disclose the amount of the fee associated with a transfer, the interest rate applicable to a loan, or the USSD charge the customer may be paying for the transaction. Sometimes they disclose via a 'url' link to a website, ignoring the fact that many users have only GSM access. Some providers only disclose prices after the customer has contracted for the service, including fees and interest rates for loans.

Advertising billboards sometimes do not even state the interest rate period but merely quote an interest rate or only give the minimum in a range (e.g., '4 per cent interest' when the rates range from 4 per cent to 6 per cent). Customers then assume the rate quoted applies, and have no awareness of whether they are being charged based on a value for a month or a year. Proper disclosure should show the total effective cost of credit, including an annual percentage rate and one-off and recurring fees, as illustrated in Table 1.

As a result, some countries have developed rules as to what must be disclosed and when it must be disclosed to potential customers. For instance, in Tanzania the Electronic Money Regulations 2015[112] require disclosure of fees and charges before imposing them.

In addition to the price of the financial services (e.g., fee for an inquiry, a transfer or transacting a loan), in many markets, there is a lack of transparency when it comes to the charges for the underlying telecommunication service (principally USSD) that customers use for those mobile financial services. When accessing a provider that is not the MNO, the customer may not even know whether the MNO is charging him or her – or the provider – for the session. Some MNOs inform the customer of the charge after the transaction, and others do not inform the customer at all.

---

111 Mazer, Rafe and Rowan, P. (2015), *Competition in Mobile Financial Services, Lessons from Kenya and Tanzania*, CGAP.

112 The Bank of Tanzania Electronic Money Regulations (2015), Part XI, provide: "(1) An electronic money issuer shall display and disclose charges and fees for its services to its customers and any changes thereof. (2) An electronic money issuer shall notify its customers the fees and charges before imposing such fees or charges. (3) The notice to customer shall (a) be delivered through electronic media and displays in a conspicuous place at the electronic money issuer's offices and agents outlets; and (b) not be misleading to customers;".

Table 1. Basic consumer disclosures in mobile financial services

Poor disclosure	Better disclosure
"Your loan request of **** has been approved and funds credited to your account."	"You will receive ****. The annual interest rate is **% in addition to a fee of ****. You will make 3 weekly payments of: **** and repay a total amount of ****. Your first payment is due 7 days after you receive your loan. Early payments are welcome. Your next payment of **** is due on 8 July 2016. Please confirm you agree to these terms by pressing 1."

3.7.2 Privacy, data protection and security

The lack of access to formal financial services in developing countries makes consumers more likely to consent to access to and use of their data, and less aware of the risks. Consumers also often do not have the support of well-tuned legislation, much less enforcement by courts or other agents. Breaches of privacy and particularly data security may result in identity theft, harm to credit records, fraud and other risks. Poor people thus tend to be more vulnerable than those in well developed markets.

A range of privacy and data protection issues will need to be addressed in most mobile financial services markets. These include requirements to obtain effective consent, including through 'opt-in' permissions for use of customer data. Such rules on data sharing and use of data by the provider for recurring purposes would place greater responsibility in the hands of consumers for how their data is used. Rules on liability for third party use of customer data need to be developed. Privacy and marketing rules may be needed as well.

Privacy and data protection laws will generally need an overhaul in many countries that have as yet only rudimentary legislation. They may rely extensively on recent data protection adopted in the European Union.

Box 10. Data protection in the European Union

The recently revised European General Data Protection Regulation[1] applies to the processing of personal data of data subjects in the EU, regardless of the location of the data controller and/or of the data processor. It clarifies the concept of personal data. Importantly, it strengthens the obligations imposed to organisations, such as the appointment of 'data protection officers', performance of 'privacy impact assessments', adoption of security and data protection policies and procedures, as well as the obligation to notify data breaches to the competent authorities and, in certain cases, to the data subjects. Further, it defines more demanding requirements regarding the information to be provided to the data subject as well as the data subject's consent. Controversially, it includes the right to be forgotten. It also establishes rules on profiling, and authorises very substantial fines for non-compliance, which may be of up to 20 million Euros or up to 4 per cent of the worldwide annual turnover.

[1] REGULATION (EU) 2016/... OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation): http://data.consilium.europa.eu/doc/document/ST-5419-2016-REV-1/en/pdf

However, lack of understanding of the data ecosystem and associated risks, as well as the appetite to access the service, likely reduce the protection afforded by effective consent systems. Regulators will likely need to ensure some basic protective measures, and increasingly focus on requiring at least the larger providers to adopt the 'Privacy by Design' principle. The development of industry standards, in dialogue with the regulators, for this purpose, will be important to ensure actual adoption.

Increasingly, the possibility for customers to 'port' their data to different firms, e.g., to support a loan application or open an account, may be considered (see section 3.6). This would empower consumers, but must be balanced against the importance of encouraging development of proprietary data analytics and innovative services.

Lastly, security issues are crucial both for consumer confidence that will drive adoption rates up, as well as for protection. Issues relate to access control, authentication, non-repudiation (i.e., preventing customers denying transactions they have carried out), data confidentiality communication security, data integrity, availability and privacy.

ITU[113] has adopted recommendations regarding security of mobile financial services. These set out approaches to system security for mobile commerce and mobile banking provided over next-generation networks (NGNs)[114] and general architecture of a security solution for mobile commerce and mobile banking in the context of NGN, including identifying relevant participants and their roles, as well as operational scenarios and implementation models.[115] It has also developed toolkits on security that are applicable to mobile money.[116]

3.7.3 Disputes and complaints processes

Processes for redressing customer complaints about the collection and use of incorrect data, or data incorrectly collected, will be needed. Disclosure about what data about a customer is collected, how it will be treated and used, including for third parties, will also need to be developed.

The need for such processes is not merely for data matters, however. Dispute and complaints procedures are important to protect consumers and ensure trust in the mobile money system.[117] Mobile money providers often provide free customer service hotlines and communication channels. Digicel reportedly doubled its call centre staff in Haiti on paydays for the Ti Maman Cheri Program.[118] It can also generate feedback from customers, as seen in the LEAP Program in Ghana.[119] In Colombia, Banco Davivienda trains and employs former recipients of government-to-person payments to support the hotline and to encourage reporting of complaints and improve resolution.[120]

---

113 ITU-T Study Group 13 on Future Networks.

114 Recommendation ITU-T Y.2740.

115 Recommendation ITU-T Y.2741.

116 ITU-D Study Group 2, Question 17-3/2 on progress on e-government activities and identification of areas of application of egovernment for the benefit of developing countries.

117 CGAP, March 2016, Zimmerman, J. and Baur, S., *Understanding How Consumer Risks in Digital Social Payments Can Erode Their Financial Inclusion Potential*: www.cgap.org/sites/default/files/Brief-Understanding-How-Consumer%20Risks-in%20Digital-Social-Payments-March-2016.pdf

118 Zimmerman, Jamie M., and Kristy Bohling. 2015. *Partnering with Existing National Safety Nets for Emergency Payments: WFP's Collaboration with the Pantawid Pamilyang Pilipino Program in the Typhoon Haiyan Response*. Somerville, Mass.: Bankable Frontier Associates, April.

119 Abbey, C. O., E. Odonkor, and D. Boateng. 2014. *A Beneficiary Assessment of Ghana's Cash Transfer Programme (LEAP) in May 2014*. Accra: African Development Program Ghana.

120 CGAP. 2014. *Going Mobile with Conditional Cash Transfers. Insights and Lessons from the Payment of Familias en Accion through DaviPlata Wallets in Colombia*. Working Paper. Washington, D.C.: CGAP.