Ethiopian's New Payments Sector Regulations (Part II)

By: Fekadu Petros
Fekadu Petros & Partner Law Office
25 October 2020

Payment instrument issuer regulation

Payment instrument issuers are either regulated financial institutions or non-financial institutions which are subject to special issuer regulation. Ethiopia's payment instrument issuer directive, i.e., Licensing and Authorization of Payment Instrument Issuers Directive No. ONPS/01/2020 (hereinafter Issuer directive) came into force on 1 April 2020. The Issuer directive is the first directive issued with the view to implementing the National Payment System Proclamation No.718/2011, ten years after the proclamation was promulgated. Apparently, Ethiopia has taken very long to determine key policy issues such as the choice between bank-led and non-bank led mobile money system; and the choice between opening and not opening the sector to foreign investors. It finally opted for a non-bank led system, and this more liberal approach seems to result from two considerations. First, the winds of liberal reforms undertaken by the Ethiopian State following the ideological reorientation of 2018 could only lead towards a liberal direction. And, the issuer directive is partly the result of these developments. Secondly, non-bank based mobile money system (such as a mobile network operator led system) is superior in terms of meeting the much needed financial inclusion objectives than the bank led model. While banks can also offer mobile money services, their high cost structures make it difficult to serve low-income customers in a sustainable manner. Mobile money is a low-margin/ high-volume business, requiring a set of capabilities and mindset which traditional banks are not well positioned to embrace.

The strengths of MNOs in providing mobile money services can be summed up into three reasons:

i. MNOs have a number of assets they can leverage to offer mobile money services. In addition to their experience with airtime distribution, the SIM card and data channel on customer handsets give users and third parties an interactive interface at a very low cost;

ii. MNOs bring a number of skills that are both central to their core business and necessary for mobile money, including expertise in mass marketing and building and managing a broad distribution infrastructure; and

iii. MNOs use mobile money to cross-sell new services to customers they already serve and to compete for customers on other networks enhancing their competitive advantages.

On the question of foreign providers, Ethiopia has opted for the sector to remain reserved to domestic investors. As foreign investor under Ethiopian financial sector law encompasses foreign nationals and any entity whether or not incorporated in Ethiopia with foreigner ownership, the restriction is very stringent. From this perspective the government's act of inviting foreign bidders to buy equity from the state owned Ethio telecom appears to be paradoxical. Part of the reason why Ethio telecom is an attractive investment is the potential to get into digital financial services industry.

Licensing and authorization requirements

The main requirements for getting license as Payment Instrument Issuer pertain to minimum capital and fitness and propriety test for officers (i.e., directors, and senior executive officers). Before dealing with these requirements however, it is important to look into the requirements for existing financial institutions and requirements for new applicants for license. For the later group the whole range of requirements apply.

Licensing vs. authorization: some terminological confusions

The directive stipulates that existing financial institutions, that is, banks and MFIs do not need to apply for license. They need to apply for only authorization. At this juncture, one may ask what is 'authorization' and how is it different from 'license'? While many terminologies pervade market entry regulations throughout the world, the Ethiopian legal system uses registration and license as the standard requirements. However, the payments system regulation is replete with terms 'license', 'authorization', and 'approval'. While license means permission to enter a market and supply goods and services, authorization and approval seem to be peculiar to the financial services industry, at least in Ethiopia. A cursory reading of the NPS proclamation and the Issuer directive suggest that there is confusion in the way these terms are used breeding ambiguity and unpredictability in the regulatory environment.

First, the NPS Proclamation confuses authorization for license. Throughout the proclamation the term ‘authorization’ is used to refer to the institution being allowed to do a particular financial services business, not about a particular product. Hence, the proclamation uses the term ‘authorization’ interchangeably with ‘license.’ In contrast, however, the Issuer directive assigns different meanings to ‘licensing’ and ‘authorization’- licensing as a requirement for new market entrants, but authorization for existing ones, i.e., for specific products developed by existing companies.

Secondly, the Issuer directive confuses ‘authorization’ and ‘approval’ or uses them interchangeably. Essentially, there is little problem in using these two terms interchangeably: if both relate to product, i.e., approval/or authorization of a specific product. The confusion is not that innocuous however, as the proclamation also confuse ‘authorization’ with ‘license’.

The confusion between authorization and license is more problematic. License is given to the Issuer in general terms to perform payment instrument issuing business. Once licensed, an Issuer needs authorization before it introduces specific products on the market. In other words, an issuer that wants to introduce a new instrument must get, not a license, but the authorization/approval for that product. Such a product/service specific regulation is not unique to the financial sector alone. A few sectors require such draconian product/service specific requirements in Ethiopia.

One of the anomalous requirements arising from the confusion of ‘license’ with ‘authorization’ is the procedure of piloting under Section 4.10-4.14, where the NBE can test a new instrument before its commercial launch. What is abnormal about this provision is that it also requires licensing of an Issuer to be pilot-tested. Normally, the licensing (formation) of an Issuer of instrument cannot be the subject of piloting. However, the specific financial products which an issuer plans to introduce can be pilot-tested. In other words, piloting is not an entry regulation; it is product specific regulation and should come as a post entry regulation. On the other hand, none of the payment system regulations mention the requirement of commercial registration which is otherwise a mandatory requirement for any business in Ethiopia. Therefore, even though the NBE directives do not mention the requirement to do commercial registration, one must first obtain certificate of commercial registration before it applies for license at the NBE, at least as far as the Ethiopian law is concerned.

Minimum capital requirement

Generally, minimum capital requirement is one of the prominent features of the financial sector regulations. It is a prudential requirement aimed at preventing insufficiently capitalized players from getting into the market, and posing risk to the system. Accordingly, the Issuer directive sets a minimum capital of 50 million Birr, which is 10% of the minimum capital required for banks. While almost all jurisdictions require non-bank mobile money issuers to meet initial minimum capital requirements to receive a license to operate such a requirement has both prudential and non-prudential objectives. Overall, a minimum capital requirement can serve the three overlapping functions, namely the guarantee function, organizational function, and screening function: (1) it stipulates what assets the provider must hold as a minimum requirement to insure creditors (including depositors) from insolvency risk and minimize subsequent system disruptions (guarantee function); (2) it ensures that the institution can cover operational costs, such as the infrastructure, management information system (MIS) and start-up losses to reach a viable scale (organizational function); and (3) it aims to set a cost that creates a barrier to market entry for new institutions that want to pursue the business initiative (selective function)

Besides setting the minimum capital requirement, the directive also prescribes dispersion of ownership of shares. It states that at least there shall be ten shareholders, and the maximum amount of one shareholder to be 20%- a typical pro-dispersion policy, and share company as a form of organizing an issuer business. These provisions mirror the requirements in all other financial institutions in Ethiopia.

Operational regulation

The term operational regulation is meant to cover all the regulatory and compliance issues that arise after licensing of an Issuer. These post entry regulations can be classified into three broad categories: prudential requirements, cardholder protection and anti-money laundering standards. Let us now turn to each of these in detail.

Prudential requirements

Payment Issuers are subjected to prudential supervision under the Issuer directive. Prudential regulation entails close on sight and offsite supervision of an entity with the aim of ensuring the soundness its operations and its overall health. The application of prudential regulation has

traditionally been limited to banks, and other deposit taking institutions, or institutions that pose systemic risk to the economy. In the payments sector, the volume of payments being made out of, and into, bank accounts adds a strong incentive to impose prudential regulation more evenly on all significant participants. Experiences of many countries show that regardless of whether or not the chosen mobile money system is bank-based a sustainable payment system requires some level of prudential supervision. The importance of prudential supervision to payments service providers has been justified on the following considerations:

i. the payments function is essential to the smooth operation of the national financial and commercial sectors;
ii. it is a big business; while profitable for its participants, is not necessarily being operated efficiently from the public perspective;
iii. most new payment services are not regulated by, or performed subject to, the terms of any public law of general application that ensures consistent standards of disclosure, and
iv. payments services may be the medium for the spread of systemic risk and loss to the public if a failure by one financial institution may be transmitted to others.

In any case, the level of prudential regulation imposed on Issuers and other payment system participants should be less severe than that applied on banks. This is so because, banking regulation imposes capital requirements and other prudential requirements on banks that have no close analog in the nonbank world. In exchange, banks serve as the exclusive providers of certain financial services such as deposit-taking and commercial lending funded from that deposit-taking.

The first and foremost prudential requirement in the Issuer directive is those pertaining to the qualifications and character of its management- often dubbed as –'*fitness and propriety requirement*.' Fitness and propriety requirement remains the hallmark of financial sector regulation in Ethiopia. All the directives issued by the NBE in respect to licensing of all other financial institutions invariably require that the directors and senior officers meet minimum character as well as educational qualifications. The fitness and propriety of officers of Payment Issuers are moderate compared to the requirements for other financial institutions. These requirements are listed under Section 5 of the directive: minimum of first degree is required for directors, chief executive officers and senior executive officers; a minimum of ten years work experience is required for CEO, and 8 years for senior executive officers. In terms of character directors and officers of issuers are required to be of good reputation, honest and diligent. This is

to be attested by absence of record of criminal conviction or absence of record of violation of administrative regulations such as withholding information when requested by a public authority.

Besides, the fitness and propriety requirements, the Issuer directive prescribes prudential requirements primarily in respect of the electronic money flout management. The electronic money flout is defined in the directive as 'the total outstanding value of electronic money issued by a payment instrument issuer that may also be reflected by a cash deposit in a bank or a government security or both.' Section 10 the directive requires that the entire amount of the electronic money flout should be either deposited in a bank (with written permission of the NBE), or invested in safe government securities (such as bonds and treasury bills). Section 10.3 states that the amount (of the electronic money flout) belongs to users (customers) and is to be managed by the issuer on their behalf. The implication is clear. Unlike banks that own money deposited by customers, payment issuers do not own the funds in the electronic money flout account. This is further reinforced by sub-section 9, which requires the issuer to transfer 80% of the interest earned on the account to the customers, with prior approval of the NBE about the manner of distribution.

Another important prudential requirement is that which regulates the customers' maximum transaction and account limits. The rationale behind this provision is the policy of keeping mobile and digital banking as a low value money transfer system-since unless limited in this way the large number of transactions can pose great risk on the financial system.

Thus, Section 8 introduces three levels of customer accounts.

- Level 1 account shall be subject to a maximum account balance of Ethiopian Birr 5000, and an aggregate daily transaction limit of Ethiopian Birr 1000, and aggregate monthly transaction limit of 10,000.
- Level 2 accounts shall be subject to a maximum account balance of ETB 20000, an aggregate daily transaction limit of Ethiopian Birr 5,000 and an aggregate monthly transaction limit of Ethiopian Birr 40,000.
- Level 3account shall be subject to a maximum account balance of Ethiopia Birr 30,000, an aggregate daily transaction limit of Ethiopian Birr 8,000 and an aggregate monthly transaction limit of Ethiopian Birr 60,000.

Users cannot circumvent the limits by opening more than one account. To this end, Section 8.2 and 8.3 prescribe that if a user owns more than one account in the same level, the

limitation for one account applies disregarding the others; and if a user owns more than one account in different levels the limitation for the higher level applies disregarding the lower level(s).

The directive does not impose account and transaction limits for business customers. However, sub-section 8.7.e limits the merchant's ability to withdraw its entire balance in cash. Though how much the merchant can withdraw is not shown in this provision, it will be part of the overall agreement to be made between the Issuer and the merchant. The other transaction limit pertains to over-the-counter transactions. Hence, for a walk in customer the directive imposes a transaction limit of 500 Ethiopian Birr. The objective seems to be to discourage OTC transactions.

To ensure compliance with these prudential requirements the directive introduces strict reporting obligations. Thus daily reporting obligation is imposed on Issuers in section 10.5 for ensuring that the balance in the electronic money flout account matches the sum of individual electronic accounts maintained by customers. And, a long list of records for quarterly reporting is stipulated in Section 13.2 including statistical data on customers and accounts, customer complaints and data security challenges. All this is meant to ensure the safety and soundness of the issuer's business.

Finally, the issuer directive also imposes IFRS compliance obligation as an accounting and financial reporting format. Section 13.3 and 4 impose two obligations on Issuers. One is issuers are required to record their financial statements in accordance with IFRS. Secondly, Issuers are required to get their financial statements audited by authorized, independent external auditors and submit the report to the NBE within two months. In a way this was not necessary. There is already a proclamation requiring share companies to follow an abridged version of IFRS, i.e., Accounting and Financial Reporting Proclamation No. 847/2014.

Consumer/ Card-holder/ protection

Customer protection is the other major objective of the issuer directive. The directive stipulates customer protection in two ways. One is protection of the customer funds, and the other is regulating the issuer-customer agreements. In respect to the customer fund protection, even

though banks serve as the ultimate custodians of an issuer's pooled accounts, the banks and the issuer are subject to the same general type of consumer protection regulation because the issuer maintains pooled accounts on behalf of its customers. The nature of electronic money system poses three major types of risks to customer funds, which the directive sets out to address. These are: insolvency risk, liquidity risk and operational risk. First and foremost, if the e-money Provider or bank where the Provider holds its customers' funds becomes insolvent, customers bear the risk of not being able to recover their funds ('insolvency risk'). The funds may be used to repay privileged creditors, or distributed proportionately among ordinary creditors of the insolvent institution (while naturally depositors should have been insulated from bankruptcy). Second, customers may not be able to cash out their e-money accounts upon request ('liquidity risk'), if the ratio between e-money issued and customers' funds is greater than 1: 1. Regulation should thus safeguard customers' funds by constraining the Provider from using those funds for its own purposes. Third, customers' funds may be lost due to 'operational risks' such as fraud, theft, misuse, negligence or poor administration.

On the international plane, various proposals have been made to identify and harmonize the efforts to tackle consumer risks in the digital financial services sector. To this effect, the Consultative Group to Assist the Poor (CGAP) and United Nations Capital Development Fund's ("UNDCF") have identified the following specific areas for regulatory focus:

(i) fraud types that have potential negative effects on customers, such as SIM swaps and card skimming;
(ii) (ii) breaches of data privacy and protection, as inadequate data handling can trigger other risks such as identity theft, misuse by government, sale of one's data without knowledge or consent, etc;
(iii) (iii) agent misconduct that causes financial loss, poor service quality, or mistrust in the agent network; and
(iv) (iv) ineffective or inadequate consumer recourse and its effect on consumer trust as well as financial services uptake and usage.

Another source of risk for consumers in the digital financial services ecosystem emanates from the participation of non-financial companies that are not regulated by prudential regulators. Given the technology intensive nature of payment services, providers often procure vital technological infrastructure from non-financial companies through partnerships. However, these

partnerships bring new, and previously unregulated players into the digital financial services space. Regulators need to determine whether consumer protection frameworks which focus on disclosure requirements and consumer recourse mechanisms apply to the new players.

In general all the foregoing customer protection requirements can be summed up into four specific obligations, namely, fund isolation, fund safeguarding, customer data protection and general obligations towards customer fair dealing. The Issuer directive covers all these four areas to a fairly sufficient degree.

The purpose of fund isolation being prevention of comingling with own funds, it is aimed at protecting customer funds from being claimed by creditors of the issuer in situations of issuer insolvency. Section 10.12 introduces this principle stressing that the 'Issuer shall segregate its own funds from that of users.' In addition, Section 15.2 provides that the 'issuer shall safeguard funds of a user of payment instrument by not making them comingled at anytime with the funds of third parties and making them insulated against the claims of other creditors of the payment instrument issuer.' While fund isolation can serve the function of safeguarding also, they are not always the same. Fund protection is broader in scope referring to the overall obligation of the issuer to be prudent in the management of customer funds such as by depositing it in a bank, and procuring deposit insurance

Customer data protection is one of the vulnerabilities of the digital environment. So much so that, the directive prescribes Section 12 about confidentiality obligation, announcing service interruption times, establishing customer call center, and obligation of reporting cyber security breach and data loss. Section 12 of the directive also provides broader obligations of fair dealing towards customers such as the use of standard terms and condition which can only be amended with the prior consent of the NBE, announcing list of its agents, and putting in place effective complaint handling and dispute management system.

Anti-Money Laundering (AML) requirements

AML and CTF standards require financial institutions to verify the identity of customers before they can access financial services with the view to detecting, reporting and preventing the use of their services for money laundering and financing terrorism. Internationally, significant efforts have been made to develop guidelines and common standards for AML as money laundering has

become a global issue in the financial sector. Because of the international nature of the threat of money laundering and terrorism, the international community has established the Financial Action Task Force (FATF) which generates global standards for countries to follow. Therefore, the FATF has developed recommendations that are widely recognized as the international standard for AML/CFT rules and are the leading source of standards for Know Your Customer (KYC) and Customer Due Diligence (CDD) measures in the AML/CFT context.

In many countries AML laws are set out to meet three overarching objectives, namely, protection of financial integrity, anti-corruption and harmonization with international standards. Ethiopia's AML regulatory regime is inspired by the Proclamation 780/2013-a proclamation aiming to prevent money laundering and financing of terrorism. The proclamation was enacted partly as a response to international pressure to cooperate in AML/CTF initiatives. Currently, Ethiopia has an elaborate system for implementing AML standards including a proclamation, a regulation and a Financial Intelligence Center (FIC) which coordinates AML activities. And, all banks have created AML compliance units for overseeing AML measures.

AML policies are implemented through the know-your-customer (KYC) principles. According to Section 2.13 of the Issuer directive, KYC is defined as a set of due diligence measures undertaken by a financial institution or a payment instrument issuer including policies and procedures to identify a user and the motivation behind his financial activities. Hence, the directive introduces key KYC principles in Section 11 and 15.3. Section 11 stipulates due diligence requirements moderated by customer level category, that is, the intensity of the requirement increases with the customer level as defined in Section 8. Therefore 'for level 1 accounts, name, date of birth, residential address, telephone number, recent photo of the user suffices to meet the CDD requirements' has to be registered. And, interestingly, the directive requires neither an identity card, nor physical appearance of the customer as it prescribes that 'the user shall be introduced by another person who already maintains an account with the payment instrument issuer.' Obviously, the introducing 'other person' cannot himself be a level 1 customer for fear that if it is so allowed, a network of unidentified users may be created that can threaten integrity of the system.

For level 2 and level 3 accounts the CDD requirements, in 11.2.b and 11.2. c, respectively include 'name, date of birth, residential address, telephone number, recent photo and identity

card of the user'. These are sufficient to open and operate an account. The only difference between level 2 and level 3 in the directive is that the later can be entities and as a result business address may be required instead of a residential address. Given that the directive provides separate CDD requirements for merchants under 11. 2. d, one may wonder the apparent inconsistency. The two provisions can be reconciled if one interprets 'entities' to mean non-commercial entities like NGOs. For merchants and agents (which are merchants by definition) CDD requirements comprise 'memorandum and articles of association (where applicable), business license, tax payers' identification certificate, (where applicable) bank account information (where applicable), the name of the owner, business address, owner contact information, and information of employees of the merchant.' A walk-in-customer is however, subjected to level 2 requirements. The explanation for this can be the policy of discouraging over-the-counter services and customers.

Section 15.3 reinforces the CDD obligations of Issuers prescribing that issuers shall identify their accountholders, set up processes that is capable to trace transactions, effectively monitor procedures for AML/CFT prevention, and 'keep records related to the business of payment instrument issuance in acceptable forms for a period allowed by the relevant proclamation.' All these provisions are in accord with the AML/CFT Proclamation.

Conclusions

Even though Ethiopia is late in modernizing its payments system laws, the recent reforms are profound in terms of the liberalization and its potential impact on financial inclusion. While the measures taken so far fall short of allowing foreign investor participation in the financial sector, whether this is a long term policy remains to be seen. An important consideration in this regulatory experimentation is the development of regulatory capacity at the level of the NBE. This is indeed an urgent question that needs to be resolved. Only with enhanced technical knowhow can the NBE effectively regulate the participation of fin techs in the provision of digital financial services, and put in place appropriate customer data protection standards.

The current regulatory relaxation has allowed some degree of liberalization in the areas of financial technology provider participation as it allows outsourcing of vital segments of issuer services, and issuer-fin tech partnerships. This is not unique to Ethiopia; in the digital payments industry outsourcing has become a key business model. The experience in many countries shows

that by outsourcing technology intensive services, Issuers can focus on implementing their core business models. As part of a larger trend to outsource technology-related functions in financial services, all but the largest banks are increasingly outsourcing processing activities to nonbanks. Issuers generally outsource these services when specialized companies have a comparative advantage due to expertise or economies of scale. This can reduce operating costs and avoid large, fixed-cost investments in processing technology.

While unfettered partnerships and outsourcing can give rise to regulatory arbitrage, a balanced regulation that promotes efficiency needs regulatory capacity to identify the right circumstances and to respond appropriately to issuer-fin tech relationships that abuse the system. Without adequate knowledge, there can only be skewed regulations either because the market will be unruly out of absence of regulation, or the market will be stifled due to excessive regulations driven, among other things, by fear. Regulatory interventions driven by fear of arbitrage can unnecessarily stifle the sector and hinder development-and hence, hamper financial inclusion and modernization.

Abuse and unauthorized use of customer data is the other problem of modern payments market place. While modern payments services has resulted in the shift of customer data control from merchants to tech companies, in Ethiopia the recently issued Financial Service Consumer Protection Directive has resolved many of these problems.