CGAP

WORKING PAPER

Regulatory Framework for Digital Financial Services in Côte d'Ivoire

A Diagnostic Study

Patrick Meagher

November 2017

Acknowledgment and disclaimer: This diagnostic study is based largely on a desk review, with information and guidance provided by Estelle Lahaye, Corinne Riquet-Bamba, and Stefan Staschen of CGAP. Discussions with and insights gleaned from market actors in Côte d'Ivoire and Senegal were particularly helpful. Responsibility for the information and views set out in this paper lies entirely with the author.

Suggested citation: Meagher, Patrick. 2017. "Regulatory Framework for Digital Financial Services in Côte d'Ivoire: A Diagnostic Study." Working Paper. Washington, D.C.: CGAP.

TABLE OF CONTENTS

ACRONYMS V

EXECUTIVE SUMMARY VI

1. INTRODUCTION 1

2. OVERVIEW OF DFS MARKET CONTEXT 3

2.1 Market development 4

2.2 Market infrastructure 6

3. E-MONEY AND PAYMENTS 7

3.1 E-money: Regulatory definition and treatment 7

3.2 Protection of funds 9

3.3 Issuers: regulatory requirements 10

3.4 E-commerce, e-signature 11

3.5 Payments 12

4. USE OF AGENTS 15

4.1 E-money 15

4.2 Transfers 17

4.3 Agent banking 18

5. CUSTOMER IDENTIFICATION 20

5.1 Identity documentation 20

5.2 Know Your Customer 21

5.3 KYC tiering 23

6. CONSUMER PROTECTION 24

6.1 Transparency and conditions of services 24

6.2 Complaint channels 27

6.3 Client data protection 28

7. COMPETITION AND COORDINATION 29

7.1 Interoperability 29

7.2 Channel access 30

7.3 Regulatory responses 30

8. CONCLUSION 33
8.1 E-money and payments 33
8.2 Use of agents 34
8.3 Client identification 34
8.4 Consumer protection 35
8.5 Competition and coordination 36
SOURCES CONSULTED 38
LEGISLATION CONCERNING DFS IN WAEMU AND COTE D'IVOIRE 40

ACRONYMS

ARTCI	Ivoirian telecom regulator (*Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire*)
ATM	Automatic teller machine
BCEAO	Regional central bank (*Banque Centrale des Etats de l'Afrique de l'Ouest)*
CENTIF	Financial Intelligence Unit in Côte d'Ivoire (*Cellule Nationale de Traitement des Informations Financières*)
DFS	Digital financial services
EME	E-money issuer that is not a financial institution (*Etablissement de Monnaie Electronique*)
FCP	Financial consumer protection
FI	Financial institution
FIU	Financial Intelligence Unit
GIM-UEMOA	Regional payments switch (*Groupement interbancaire monétique de l'UEMOA)*
IOB	Type of bank agent used in Côte d'Ivoire (*Intermédiaire en Opérations de Banque*)
KYC	Know your customer
MFI	Microfinance institution
MNO	Mobile network operator
NBFI	Nonbank financial institution
OTC	Over the counter
P2P	Person-to-person
POS	Point of service (device)
SICA-UEMOA	Regional payment and settlement system (*Système Interbancaire de Compensation Automatisé dans l'UEMOA*)
STAR-UEMOA	Regional wholesale payment system (*Système de Transfert Automatisé et de Règlement* dans *l'UEMOA*)
USSD	Unstructured supplementary service data
WAEMU	West African Economic and Monetary Union (UEMOA)

EXECUTIVE SUMMARY

Regulation plays a critical role in the development and spread of digital financial services (DFS). This paper offers an analysis of the regulatory framework for DFS in Côte d'Ivoire, including its coverage, its conducive features, and its gaps and obstacles.

Côte d'Ivoire is a regional leader in DFS, particularly in the use of mobile money. It is a lower-middle-income country that has nearly 8 percent annual GDP growth. It has a high rate of mobile phone penetration (estimated at 113 percent), and a more modest rate of formal financial inclusion (46 percent of adults, including bank, microfinance, postal, and mobile money accounts). Mobile network operators (MNOs) have been the lead players thus far. They account for three of the five mobile money deployments and the majority of agents. MNOs have mainly partnered with banks that issue e-money. However, in the wake of recent regulatory changes, MNOs are moving to establish e-money subsidiaries.[1] Over-the-counter (OTC) services providers, who provide affordable transfer services to clients, including those without digital accounts, are also significant.

Any discussion of legal or policy matters in Côte d'Ivoire must pay close attention to the rules laid down by the West African regional institutions of which that country is a member. In this paper, we are principally concerned with the West African Economic and Monetary Union (WAEMU), a currency union and evolving free trade zone. The WAEMU's central bank, BCEAO (*Banque Centrale des Etats de l'Afrique de l'Ouest*), exercises exclusive authority over the money supply and is the primary authority (with the participation of the regional Banking Commission) for the regulation and supervision of financial institutions (FIs), payment systems, and digital finance.

The WAEMU Commission's jurisdiction extends to activities that may have a potential impact on the regional market, for example, in competition regulation. Member countries, including Côte d'Ivoire, retain legal authority in other areas affecting DFS, such as telecommunication (telecom) regulation and general consumer protection. Thus, for example, while BCEAO retains sole authority to regulate financial services from a financial consumer protection (FCP) perspective, countries such as Côte d'Ivoire have general consumer protection laws and oversight institutions that impact financial services.

Policy makers at the national and regional (WAEMU) level are taking steps to expand DFS access. Côte d'Ivoire has taken aim at the digital divide and is improving fiber-optic infrastructure and simplifying telecom licensing. It is moving toward a national system of individual identity numbers and is digitizing public-sector payments. A regional payments switch is in place. Financial legislation provides for an array of service tiers, including banks and other credit providers, payment companies, and microfinance institutions (MFIs). In addition, a number of basic banking services are now required to be provided free of charge.[2] Further, a regional financial inclusion strategy was adopted by the WAEMU Council of Ministers in June 2016. Côte d'Ivoire also has a national-level financial inclusion strategy.

Although supportive measures are being taken, the DFS approach in Côte d'Ivoire has not yet reached its potential. Reasons for this include significant gaps in

1 Orange and MTN have established e-money subsidiaries licensed by BCEAO (situation at the end of May 2017).

2 In the relevant instruction, the services are simply listed, but without a definition. Reportedly, as a result, some banks have changed the names of the relevant services and are charging for them.

interoperability between digital financial platforms, cash preference and other "adoption" challenges, and the regulatory obstacles addressed in this paper. This paper focuses on the implications in Côte d'Ivoire, but the challenges are often posed at the regional level. The constraints include broader policies impinging on financial inclusion, notably an interest rate cap, which will affect the provision of digital credit going forward, and a limitation on MFIs' ability to move beyond savings and credit services into other activities, such as e-money issuance.

E-money and payments

E-money. The cornerstone of DFS is the issuance of electronic money. In a 2015 instruction that updates earlier rules covering Côte d'Ivoire and the other WAEMU markets, BCEAO defines e-money as a monetary value in electronic form, issued without delay against funds in (at least) equal amount, and accepted as a means of payment by third parties.

The instruction enables issuers to accept funds from the public for purposes of e-money issuance without (simply for that reason) having to obtain a deposit-taking license. It allows for a range of e-money issuers. Banks, payment financial companies, MFIs, and e-money institutions are permitted to issue e-money with a few preconditions. Microfinance regulations severely limit MFIs' involvement in noncore activities such as e-money issuance. Other issuers, for example, nonfinancial companies, are called *Etablissements de Monnaie Electronique* (EMEs). To become licensed, EMEs must meet separate standards on corporate governance and be solely dedicated to e-money issuance. As mentioned, some MNOs are in the process of setting up (or have already set up) e-money subsidiaries to use this EME license.

Issuers must promptly deposit funds received from e-money clients in accounts specifically for this purpose at one or more banks or MFIs. This e-money "float" is to be separately identified in the accounts of the issuer and depositary institution—and the total value held by each issuer must be at least equal the amount of e-money outstanding at all times. The placement of these funds is prescribed. An issuer must place at least 75 percent of the value of all its e-money in circulation in sight/demand deposits, and the rest in specified types of investments (no trust, escrow, or similar structure is required).

Côte d'Ivoire's deposit guarantee scheme should, by its terms, cover EME float deposits up to the ceiling amount. But the scheme is not yet in operation, nor is it fully clear how it would treat e-money float in practice. The e-money instruction prohibits issuers from issuing e-money as credit and from paying interest on e-money float (but this does not prevent banks and MFIs from linking a client's e-money account to her/his other accounts—e.g., credit or savings).

The e-money instruction imposes quantitative limits on e-money holdings per client: a maximum e-money balance with a particular issuer of 2 million FCFA (~US$3,400) and a maximum of 10 million FCFA (~US$17,000) in recharges (topping-up of balance) per month across all institutions.

E-commerce and e-signature. E-money (and DFS generally) depends to a great extent on the framework for e-transactions. The critical component here is the certification of digital documents (with e-signatures) that have replaced paper documents.

There is both national and regional legislation in this area. The WAEMU regulation applies by virtue of its (and BCEAO's) predominant authority over financial services. As the domestic authority for e-commerce, the Ivoirian telecoms regulator (*Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire* or ARTCI) has jurisdiction over e-signatures in general. Both regional and national legislation provide in principle for transactions to be carried out and signatures to be made effective entirely by digital means, once a certified e-signature is in place. Both provide procedures for certification and for the registration of certification services providers.

In practice, however, it is reported that fully electronic processes for account opening are not possible in Côte d'Ivoire because hard-copy certificates are required to back e-signatures. This complicates the opening of digital accounts, and (prospectively) the conclusion of digital credit agreements.

Payments. As for payment services, a 2002 WAEMU regulation authorizes banks, MFIs, and specialized nonbank payment companies to provide these services. It places them under the supervisory authority of BCEAO. Payments instruments covered include e-transfers, bank cards (ATM and payment cards), and prepaid cards. Payment services providers must abide by the rules set by each payment system, as well as with general standards for reliability, security, and enforcement. The payments regulation does not differentiate between wholesale and retail payments. The bank-based payment systems account for most large-volume and bulk payments (as well as much of the retail payments traffic). In practice, the e-money system is focused on small-value, low-volume transactions. Payment services offered by the Post also come within the purview of BCEAO, under the 2002 WAEMU payments regulation.

Use of agents

Widespread access to agents that operate under appropriate safeguards is critical to DFS and financial inclusion, generally. Authorizing the use of agents opens up the possibility of broad distribution networks. The regulatory framework in WAEMU enables financial services providers to use agents for e-money and rapid (OTC) fund transfers, but is more restrictive with respect to agent banking. (In this paper, "agent" refers generally to distributors, retail agents, intermediaries, and other third parties that handle the outsourcing of financial services.)

E-money and transfers. The e-money instruction provides for a two-tier system of primary agents (distributors) and retail-level subagents. Those permitted to serve as primary agents are retailers and other businesses (registered companies or individuals), MFIs and other nonbank FIs, and the Post. These agents may then outsource to subagents that must be registered businesses (including individuals and companies). Services that can be outsourced to agents come under the heading of marketing and supply of services related to e-money. They include signing up clients to e-money accounts, cash-in and cash-out, and payment services. Exclusive agency agreements (i.e., requiring an agent to serve a single issuer exclusively) are prohibited.

The issuer (principal) remains legally responsible to its clients and third parties for all the services contracted out to its primary agents and for the agents' liquidity and due diligence. Thus, issuers bear primary responsibility for supervising their agent networks, with BCEAO playing a higher-level oversight and inspection role.

The e-money rules expressly grant BCEAO authority to inspect EMEs along with their e-money agents and technical services providers.

In addition, a 2015 BCEAO instruction authorizes banks, NBFIs, and MFIs to use retail agents (subagents) for rapid funds transfers—real-time OTC transfers at an authorized provider or agent (not involving any bank or e-money account of the sender or recipient). These agents (OTC providers) are prohibited from collecting funds for reasons other than OTC transfer (e.g., deposits) unless the agent is an MFI. Again, exclusive agencies are prohibited. The agents act under the comprehensive responsibility of the principal (FI) and for the principal's account.

Agent banking. Beyond the e-money and transfers setting, the scope for using agents is less clear. Agent banking has proven difficult. Banks are authorized to use agents of a type called *Intermédiaires en Opérations de Banque* (IOB), under fairly stringent conditions, by the banking law and a 2010 BCEAO instruction. These IOBs are subject to prior authorization, fit and proper standards, financial guarantees (by a principal bank), and regular reporting. Banks are responsible for direct supervision of these agents. From the introduction of the rules in 2010 until end-2016, only five IOBs have been approved in three of the WAEMU countries (none in Côte d'Ivoire). In practice, IOBs have branches and satellite offices, but the instruction does not authorize them to contract out functions to subagents (in contrast to the legislation on e-money and rapid transfers). The IOB model thus does not enable agent banking initiatives to expand financial inclusion.

For MFIs, the issue of providing credit and savings services through agents is not addressed directly. Conditions and standards for MFI agent services are not defined in legislation, but in practice they appear to be within the authority of BCEAO to set on a case-by-case basis.

Customer identification

A 2015 WAEMU directive provides anti-money laundering and combatting the financing of terrorism (AML/CFT) safeguards for the financial sector and a wide range of actors involved in relevant activities. The list of entities covered includes banks, MFIs, e-money issuers, payments and transfers companies, commercial and consumer credit providers, insurance providers, and agents that provide financial services. Know your customer (KYC) procedures are spelled out in the directive. Before any business is transacted, all covered entities must identify their clients—both individuals and organizations. This means obtaining the client's full name, place and date of birth, and primary address and verifying these by checking a valid "official document" with a photograph (to be copied) and documentary proof of address.

Identity documents. Under the AML/CFT directive, identity information is to be collected at various points and retained. This applies to opening accounts, transferring funds, and establishing a business relationship. Strict procedures are to be used where there are frequent cash transactions or any suspicion of money laundering, terrorism financing, or use of false documentation. Covered entities must continuously collect and update specified client information for the duration of the business relationship. Additional AML/CFT precautions are to be taken in the case of most e-transfers and for many transactions by occasional clients. Anonymous accounts or those under assumed names are prohibited.

Côte d'Ivoire provides for official identity documentation as a matter of national policy. Whereas identification has often proven a constraint to financial inclusion, and DFS in particular, recent efforts by the government have resulted in some 70 percent of the Ivoirian population (as of mid-2016) having official identification documents. Further, the National Office for Identification is in the process of establishing a comprehensive digital identifier system.

The Ivoirian telecoms regulator (ARTCI) sets the rules for identifying customers wishing to obtain SIM cards, internet subscriptions, and other forms of digital access. Mobile phone and internet services providers must check a valid form of identification from every individual customer and record her/his full name, place and date of birth, address (postal and physical), phone number, occupation, and details of identity document (this information is not available from a central database).

Know your customer. Striking the right balance in KYC requirements means taking a risk-based approach in which standards are graduated or tiered to accommodate financial inclusion. The 2015 WAEMU directive on AML/CFT provides some risk-based accommodation in the form of lighter-touch KYC, but does not create KYC tiers. The directive only varies the way in which ID requirements are applied it does not provide exceptions for clients without official identity documents. In its application to e-money issuers, the directive in effect nullifies the exception for small transactions under the 2015 e-money instruction.

The AML/CFT directive addresses the use of agents and the required internal safeguards. Covered entities are permitted to outsource client identification and oversight while retaining ultimate responsibility for these obligations. All covered institutions are required to train their personnel and establish control systems to ensure compliance. E-money issuers must supervise their agents and subagents, ensuring there are security and monitoring provisions sufficient to meet standards in the AML/CFT regulations.

Consumer protection

Because heightened consumer risks arise in the DFS context, there is a need for well-designed protections. Apart from general safeguards discussed earlier, there are three further important elements: (1) fair and transparent dealing, (2) channels for consumer complaints, and (3) treatment of client data.

Transparency and conduct. The 2015 e-money instruction requires the issuer and customer to sign a contract to open an account. Mandatory provisions include disclosure of the limits, risks, and caution required in using e-money and the procedures in case of fraud, loss, and claims for reimbursement. The issuer is also required to make its fee schedule easily accessible to all customers and to issue an electronic receipt for all transactions. Additional provisions are noted in other financial sector and payments regulations. The 2002 payments regulation requires the conditions for the use of payment instruments and accounts to be clearly explained to the customer and incorporated into a written agreement. The regulation limits the interval between the arrival of a payment order and the crediting of the beneficiary's account. Other basic consumer provisions appear in banking and microfinance laws—and apply to accounts accessed digitally. These include, for example, transparency in fees and codes of conduct in dealing with customers.

Standardization of these e-money and payments contracts, however, is not practiced or required. This can make comparison unduly difficult. Nor is there any requirement regarding format (e.g., length or font requirements) or language (e.g., plain language or local language). Polling of customers indicates that this is a problem area.

Côte d'Ivoire's 2013 e-commerce law provides standards on advertising, offers, contract provisions, transparency of prices (including fees and taxes), and disclosure of identifying information on the seller of goods and services. Contractual provisions and procedures for acceptance are to be spelled out clearly. Also, Côte d'Ivoire has adopted a consumer law that establishes a consumer protection commission and provides specific rules on consumer and housing finance.

A concern of special relevance to DFS is the application of consumer protections to agents. Only the e-money and rapid transfer instructions have provisions dealing to any extent regarding this. The e-money instruction requires issuers to ensure that their agents post visible, legible information, such as name and contacts, for the principal issuer. It also holds issuers legally responsible to clients and other third parties for the agent's performance. Rapid transfer subagents are to include the logo of the FIs they serve on their signage and post their tariffs at the teller windows. IOBs act under the full responsibility of the bank (the principal), which must formally undertake to repair any damage caused to third parties by its agents.

Complaint channels. Pending the implementation of the new consumer protection law, financial consumer complaints are addressed in explicit terms only in the e-money instruction. There, issuers are required to set up forums for complaint handling, for both clients and their payees. These systems must be accessible by multiple communication channels at all times, establish deadlines for resolution of claims, and track all complaints received and addressed. These requirements are not spelled out in detail. Thus, procedures are not standardized, nor are providers required to inform consumers about how their complaints are to be handled.

BCEAO's regional financial inclusion strategy envisions the replication of the *Observatoire* model. Côte d'Ivoire is establishing such an institution with the assistance of the World Bank. The Ivoirian *Observatoire* will include a consumer complaint channel and research and policy development functions. It will also allow for functional comparison between institutions that offer transfer services (including between banks, MFIs, and EMEs) and institutions offering transactions accounts (including between banks, MFIs, and EMEs).

Client data. Data protection is covered by general provisions on confidentiality and personal data security in banking, microfinance, and e-money regulations. Regional legislation on credit information bureaus contains further provisions on handling client data.

Côte d'Ivoire has adopted protections for customer data in its 2012 telecoms ordinance, the 2013 law on electronic transactions, and the 2013 personal data legislation. All of these acts are enforced by ARTCI. The laws cover types of sensitive data likely to be handled in DFS operations, such as identity, biometric, household, and legal information. The 2013 data protection law and decree require prior consent of the affected person for the collection and handling of personal data.

The 2012 telecoms ordinance requires services providers to protect personal data and ensure the integrity and confidentiality of communications. The platforms and

associated digital transmissions provided by MNOs fall as well within the authority of ARTCI and the standards on telecoms, data protection, and e-commerce (an overlap with BCEAO's authority over DFS).

Competition and coordination

The potential of DFS to increase volume, efficiency, and inclusiveness in the financial system depends on connectivity among relevant communication channels and accounts. Two important constraints in Côte d'Ivoire, as in some other settings, are uneven access to mobile communication channels and limited interoperability between competing DFS providers and their networks.

Interoperability. Early rapid growth of one DFS provider tends to defer the advent of interoperability, in turn favoring dominant actors and limiting competitive growth. Thus, an interoperability policy or scheme is often essential for competition in these markets, but in most settings, it is absent or incomplete. It is often difficult to bring about voluntary agreement on interoperability in the near term, especially where there is a dominant provider. But interoperability can emerge when market players understand the potential shared benefits of network effects. BCEAO is developing a "road map for interoperability."

DFS in Côte d'Ivoire and the WAEMU region could be described as comprising closed loops and distinct operating standards, with limited but growing interoperability. A prime example of evolving integration in the region is GIM-UEMOA, which is a regional switch for ATM and POS payments. This switch is available to EMEs across the region. MFIs in the region are slated to get access to this switch, which could also be made available to all e-money issuers. Apparently, FI issuers have not been interested. By contrast, our research found that ATMs have achieved near total interoperability, but not as much progress has been achieved with POS.

Channel access. Another typical constraint to DFS expansion arises from lack of reliable access to mobile messaging channels. MNOs control the SIM card with its identity data on each mobile user, as well as the phone's communications channels, including the Unstructured Supplementary Service Data (USSD) channel, which is used by most DFS providers.

MNOs not only provide the channel for e-banking services but they also are competitors (through their EME affiliates) of FIs that want to offer mobile financial services and of EMEs that are not affiliated with MNOs. This gives the MNOs an opportunity to price-discriminate against financial services providers that are seeking access, or even to deny access, and to favor aggregators who bring them a large volume of business. There are reports from stakeholders in Côte d'Ivoire that MNOs have in some cases denied USSD access to FinTech companies or financial institutions. In other cases, MNOs have charged a lot for access or have limited access in terms of time or connection quality. But MNOs are providing channel access to their e-money subsidiaries while restricting access to others.

Regulatory responses. The frameworks for financial, telecom, and competition regulation—at national and regional levels—provide relevant standards that might be used to address the issues discussed here. For example, the e-money instruction requires issuers to facilitate *interoperability*. There has not yet been a strong

regulatory push to ensure that different participants in DFS can play together on the same, level playing field. Most observers favor suasion over coercion. Introducing, or mandating, interoperability too early may be counterproductive—it may drive up compliance costs and technical complexity. BCEAO's objective is to ensure full interoperability when the market is ready.

ARTCI has authority to approve rates and enforce tariff transparency on behalf of MNO customers. It also regulates value-added services (i.e., adjuncts to core telephone and data services). It is responsible for enforcing the laws governing e-commerce and e-signature certification. The agency is tasked with establishing an appropriate mechanism for consumer complaints and follow-up and ensuring quality of service and effective and fair competition (in cooperation with other relevant authorities).

Clearly, ARTCI's authority over mobile providers and e-commerce overlaps with that of BCEAO. This overlap argues in favor of some framework for coordination. ARTCI is mandated to cooperate with other regulatory bodies in Côte d'Ivoire and the region to regulate competition in the telecoms and data markets. At the same time, BCEAO is authorized under financial legislation, such as the e-money instruction, to bring in other regulatory authorities to carry out joint inspections. In the DFS context, ARTCI and BCEAO have established a joint working group that is analyzing several areas of concern, including interoperability. ARTCI is also developing a framework for collaboration with the national and regional competition agencies to monitor the development of the telecom sector.

In the field of USSD access, ARTCI has a basis to intervene. The telecoms legislation states that network access, interconnection, and sharing of essential infrastructure should be provided on an equal, nondiscriminatory basis. Refusal to share essential infrastructure can be deemed anti-competitive, while dominant providers have a duty to offer interconnection. ARTCI is required to monitor conditions of access, and it may enforce access as a last resort. Denial of sale, price discrimination, and agreements in restraint of trade are prohibited.

In fact, ARTCI reports that it is now requiring MNOs to open the USSD channel to external services providers and to make public their respective access offer with a price list. ARTCI was reviewing these prices at the time of the diagnostic.

Recommendations

Most of the measures suggested are within the responsibility of regional authorities, mainly BCEAO. Recommendations that concern the Ivoirian national authorities (e.g., for some aspects of customer identification and consumer protection) are noted as such.

E-money and payments. The 2015 e-money instruction has consolidated and clarified the rules in this area. But questions remain about how supportive the rules in other, related, areas are—such as banking and e-commerce. Our recommendations are as follows:

- Reconsider the interest rate caps in force across the region. These limits are likely to constrain the offer of innovative digital credit and savings products to the unbanked. At least a partial or phased liberalization is advisable. It would be best to couple this with stricter transparency requirements, including standardized

disclosures. This step would support competition, help keep interest rates low, and make it possible to phase out rate caps. This issue is relevant to licensed banks, credit institutions, and MFIs whose loan products may become available via digital channels.

- Revise the tight limit on MFI activities beyond their traditional ones of savings and credit. BCEAO should adopt an exception, or at least a higher limit, on earnings from e-money and related activities by MFIs. Care should be taken to ensure that the rule's prudential objectives continue to be met.

- Clarify protections for e-money float funds. The e-money instruction requires segregation of float funds by the issuer and the depositary institution. The treatment of these funds in the case of the issuer's bankruptcy is not clear. Thus, requiring a trust account structure might be advisable here to insulate the float from claims by the issuer and its creditors. Also, as Côte d'Ivoire's deposit guarantee system goes into operation, its scope of coverage should be clarified to ensure adequate, equitable protection of e-money float. Adopting a system of per-client "pass-through" insurance should be considered.

- Harmonize regional and national rules on e-signature acceptance and certification, and ensure coordination and clear jurisdictional lines between BCEAO and ARTCI in this area. The key is to ensure that fully digital signatures and certifications can be routinely used—without recourse to paper documents and in such a way that is easily affordable for low-income people. BCEAO reports that work is underway on revisions to the regional payments regulation for this purpose.

Use of agents. The 2015 instructions on e-money and rapid money transfers clarified the rules on agency, and took a critical step in incorporating both primary agents and subagents. On the other hand, the conditions for agent banking appear far too restrictive for the banks, and not clearly articulated for the MFIs. We recommend the following:

- Develop uniform, or at least harmonized, agency rules and standards for financial services outreach across the board—including agent banking, e-money agents, and rapid transfer agents. A functional, risk-based approach should be adopted, in preference to the current patchwork of mostly institution-based regulation.

Customer identification. Our key question is whether the new regional AML/CFT regime sufficiently accommodates financial inclusion and DFS through tiered, risk-based KYC standards. It does not, and it adds to the patchwork of limited and conflicting due diligence exceptions. On the other hand, Côte d'Ivoire's program of expanding access to official identification documents will help ease KYC procedures and thus enhance financial inclusion. Our recommendations are as follows:

- Replace the patchwork of KYC carve-outs for small transactions (including case-by-case adjustments) with a clear, consistent set of risk-based KYC tiers. The tiers should provide comprehensive coverage of financial services, including DFS, and should provide exceptions from requirements more likely to exclude traditionally unbanked groups, such as poor and rural populations (e.g., documentation of a permanent address). General Financial Action Task Force principles in the 2015 and 2012 WAEMU legislation need to be spelled out concretely in legislation applicable at the national level.

- Coordinate identification requirements for SIM cards and DFS. One promising approach that could be explored is to carry over the same identity verification procedure used for SIM cards into the KYC process—and perhaps national identification cards and databases as well.

Consumer protection. The consumer protections applicable to DFS are improving but lack comprehensiveness and consistency. The following are our recommendations:

- Strengthen and harmonize consumer protections across the full range of DFS—including digital links to savings and credit accounts as these become feasible. Provisions on fraud, security, data protection, and bankruptcy and other contingencies should be similarly expanded. Application of consumer norms to agents should be clearer and more consistent across the board.

- Enhance transparency and comparability by requiring standardized fee information for payments accounts, or at least by introducing standard requirements for format and manner of disclosure.

- A tribunal or ombudsman for retail finance, including DFS, is also important. Côte d'Ivoire is setting up a financial sector *Observatoire* and a Consumer Commission. Explicit, specific provisions related to DFS will help to strengthen protection in this subsector. Further, the protections will be most effective if all financial services providers (not just e-money issuers, as is now the case) are required to have in-house complaint systems, and for these to offer a route of appeal to the Commission and *Observatoire*, and hence to the courts.

- There is a need to make consumer protections effective in practice through systematic supervision. As matters stand, some provisions reportedly are not applied at all by providers. Good practice here involves regulatory oversight of consumer practices as a market conduct and prudential matter.

- Data collection on consumer practices should be strengthened and systematized. Data analysis can reveal patterns of practice and risks posed by noncompliance with consumer norms and effectiveness of enforcement.

Competition and coordination. Difficulties arise from the overlaps between markets, service delivery infrastructure, and regulatory regimes. The key issues here are interoperability and access to the USSD channel. Constraints in these areas act as a drag on overall DFS development and financial inclusion. Importantly, ARTCI is now requiring MNOs to open the USSD channel to external services providers. In this area, we recommend the following:

- BCEAO, ARTCI, and perhaps the competition authorities should elaborate the framework for cooperation that they have discussed and map out a strategy for rationalizing the governance of the DFS market. Recent steps taken by the two regulatory bodies are promising in this regard.

- ARTCI, in coordination with the other regulators, should monitor MNOs for potential discriminatory pricing and service quality in USSD access because this affects DFS delivery.

1. INTRODUCTION

Regulation plays a critical role in the development and spread of digital financial services (DFS). This paper offers an analysis of the regulatory framework for DFS in Côte d'Ivoire, including its coverage, its enabling features, and its gaps and obstacles. (See Box 1 for a definition of DFS.) We discuss priority areas for strengthening and reform, to be addressed at the national level and at the level of the West African Economic and Monetary Union (WAEMU), of which Côte d'Ivoire is a member state. We aim to provide analysis that is relevant and useful to policy makers in Côte d'Ivoire and to others interested in DFS regulation and its links with financial inclusion.

Part 2 provides a brief overview of the Ivoirian context in key market and policy developments. In the four parts that follow, we review the core elements of the regulatory framework for DFS in Côte d'Ivoire (i.e., what CGAP calls "basic regulatory enablers"). We consider the provisions governing e-money issuance and the use of agents in DFS (parts 3–4)—these are necessary conditions for moving financial services into the digital realm and making them broadly accessible in this form. Next, we examine the provisions on customer identification and consumer protection (parts 5–6). Such safeguards, along with protections embedded in e-commerce and personal

BOX 1. Definition of DFS

We define DFS as the suite of financial services, potentially including both traditional and new products, offered by banks and nonbank providers through digital transactions platforms. The services are accessed by digital devices, such as mobile phones, cards used with point-of-service (POS) devices or automatic teller machines (ATMs), and internet connections. Agents play a critical role here, particularly in conversion between cash and electronic funds (cash-in, cash-out). The following key elements should be emphasized:

- A digital device—either a mobile phone or a payment card plus a POS device that transmits and receives transaction data.
- Agents—individuals, retail stores or outlets, or ATMs where customers can put cash in (i.e., convert cash into digitally stored value or make a digital payment or transfer) and take cash out (e.g., withdrawing from a digital stored-value account or receiving a digital remittance or other transfer or payment).
- A digital transaction platform (*i*) enables payments, transfers, and value storage through a digital device and (*ii*) connects to an account with a bank or nonbank permitted to store e-value.
- The offer of additional financial products and services through the combination of banks and nonbanks (including nonfinancial companies) that leverages digital transactional platforms.

Source: Global Partnership for Financial Inclusion (2016), p. 46.

data handling regulations, should strengthen security and confidence in the safety of DFS, provide for the enforcement of customer rights, and thereby encourage wider use of DFS. Part 7 covers the complex of regulatory authorities involved in this field, along with the competitive challenges that result. We look at the ongoing efforts of authorities at the level of WAEMU and the Côte d'Ivoire government in addressing these special difficulties. We conclude with a short policy review and recommendations.

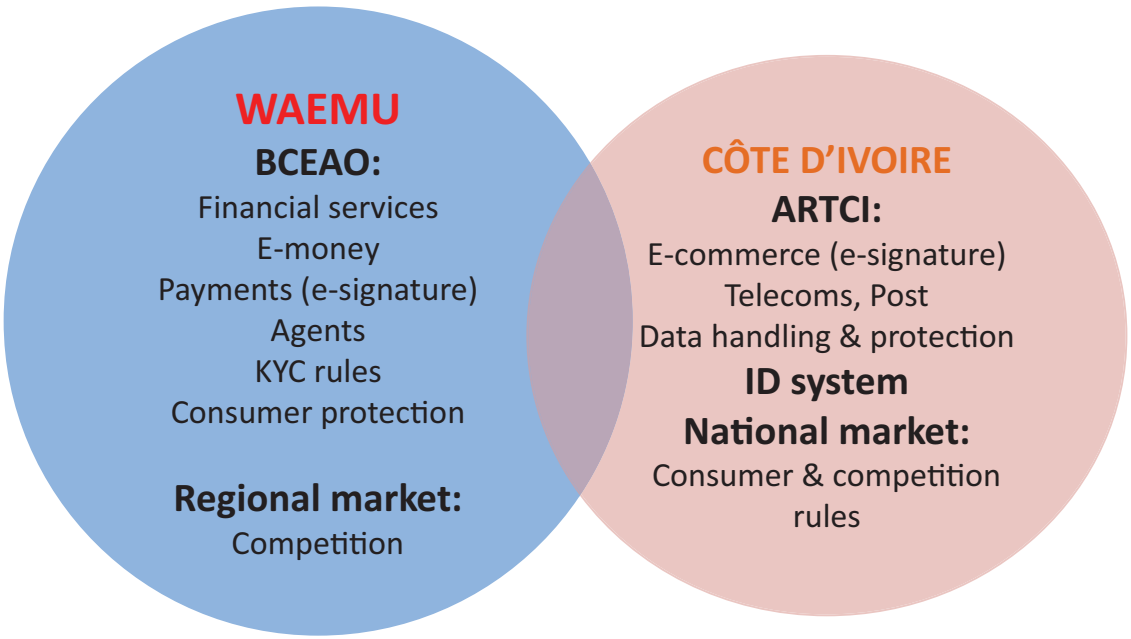
2. OVERVIEW OF DFS MARKET CONTEXT

What are the salient features of the DFS market in Côte d'Ivoire? What are some of the key features and trends in the development of this market? This discussion sets the stage for the enabling framework analysis that follows. The specific shape and modalities of DFS in practice point to specific issues in policy, law, and regulation.

Any discussion of legal or policy matters in Côte d'Ivoire must pay close attention to the rules laid down by the West African regional institutions of which that country is a member. WAEMU is a currency union and evolving free trade zone. WAEMU's leaders, acting in concert,[3] adopt legislation and policy decisions in areas such as trade, competition, finance, and monetary policy. Its central bank, BCEAO (*Banque Centrale des Etats de l'Afrique de l'Ouest*), exercises exclusive authority over the money supply and is the primary authority for the regulation and supervision of financial institutions (FIs), payment systems, and digital finance. A Banking Council has overall responsibility for the financial sector, and the region's Ministers of Finance. It also participates in decisions—but ongoing regulation and supervision are handled mainly by the Central Bank, with the participation of the Banking Commission. (See Figure 1.)

Thus, regional institutions have primary authority for the financial sector and monetary policy, as well as for regulation of activities that may have a potential impact on the regional market, for example, in terms of competition (including aspects of consumer protection). The member countries, including Côte d'Ivoire, retain legal authority in other areas affecting DFS, such as telecom regulation and general consumer protection. For example, while BCEAO retains sole authority to regulate financial services

FIGURE 1. Regulators of the DFS space: Regional and national



3 I.e., acting through the Union's Conference of Heads of State and Government and its Council of Ministers.

from a financial consumer protection (FCP) perspective, countries such as Côte d'Ivoire have consumer protection laws and oversight institutions that impact financial services.[4]

2.1 Market development

Côte d'Ivoire is a regional leader in DFS, particularly in regard to mobile money. It is a lower-middle income country that has nearly 8 percent annual GDP growth (in the wake of civil conflict). It has a population of 22.7 million; nearly half of the population lives in rural areas. It has an adult literacy rate of 41 percent. An estimated 18.3 percent of the adult population holds a bank account, according to BCEAO (at end 2015). Including microfinance, postal, and mobile money accounts,[5] the rate of financial inclusion is 46 percent, according to a BCEAO estimate. Mobile-phone (i.e., SIM card) penetration is quite high, at 113 percent, as compared to the 14.6 percent rate of internet access (Koné 2016).[6]

In terms of DFS, the number of mobile money subscribers is an estimated 10.4 million; 41 percent of these accounts have been active in 2015. Mobile money transactions in 2015 were reported to be a total of 3.8 billion FCFA (US$6.3 million). Côte d'Ivoire is the leading mobile money market in WAEMU. According to BCEAO, at the end of 2015, Côte d'Ivoire represented 41 percent of the total mobile-money registered customers in the region; 46 percent of the total transactions in volume and 51 percent in value. Côte d'Ivoire also has the largest volume of cross-border remittances in the region, reflecting its sizeable immigrant population. There are an estimated 20,000 mobile money agents in Côte d'Ivoire compared to over 900 branches of FIs and 832 ATMs. Mobile network operators (MNOs) have been the lead players thus far. They account for three of the five mobile money deployments and the majority of agents. The MNOs have mainly partnered with banks that issue e-money. However, in the wake of recent regulatory changes, two of the three MNOs have now moved toward establishing e-money subsidiaries.

Although policy makers at the national and regional level are taking steps to expand DFS access, Côte d'Ivoire has not yet seen this sector reach its full potential. Reasons for this include the limited attractiveness of DFS offers to date, relatively high costs of service, cash preference and other "adoption" challenges, and regulatory constraints. This paper focuses on the implications in Côte d'Ivoire, but the challenges are often posed, and relevant policies adopted, at the regional level.

Several positive developments in the direction of expanding access are worth highlighting. Regional financial legislation that provides for an array of service tiers, including banks and other credit providers,[7] payment companies, and MFIs (*Systèmes Financiers Décentralisés-SFD*[8]), is in place. The MFI law replaced earlier legislation that was based on a mutualist model and had a more flexible arrangement. In addition, several basic banking services are now

4 Côte d'Ivoire is also a member of the Economic Community of West African States (ECOWAS), which operates parallel to WAEMU and adopts policies to support the regional market. For example, the ECOWAS policy on e-transactions was adopted into law by Côte d'Ivoire in 2013.

5 E-money delivered by mobile phone, including the most basic handsets.

6 Note d'information n°48, Décembre 2016, BCEAO.

7 The legislation provides for a category of *établissements de crédit* that includes banks and *établissements financiers à caractère bancaire*.

8 In this paper, "microfinance institutions" (MFIs) is used generically.

required to be provided free of charge.[9] Further, a regional financial inclusion strategy was adopted by the WAEMU Council of Ministers in June 2016. Côte d'Ivoire has a national-level policy on this.[10]

Legislation on e-payments (2002), and especially e-money (2006), prompted DFS innovation, with payments, transfers, and airtime recharges ("first generation" products) being offered by bank-MNO partnerships and the development of cross-border remittance corridors. A series of regulations adopted in 2012–2015 have helped to clarify the respective roles of telecoms, FIs, and others in this sector.

During the latter period, the MNOs' search for new sources of revenue led them to move increasingly into the mobile money sector. Orange has emerged as the dominant provider in Côte d'Ivoire, accounting for at least 70 percent of overall mobile money transaction value, over half of all mobile money customers, and thousands of agents (at least 11,000 total, 7,500 active at end 2015). In 2016, Orange Money and MTN established affiliates that are now licensed as e-money issuers under the new regulation adopted in 2015.

Non-MNOs have a foothold in this market as well. Among (nonbank) e-money issuers, the two non-MNO competitors are a payments company and an MFI. The MFIs apparently have an interest in going digital, but face obstacles including deficits in human resources and a customer base that may not be big enough to justify the investment. (MFIs also face the constraint posed by a regulatory limitation on noncore business revenue.)

Also significant are OTC services providers,[11] who furnish affordable transfer services to clients, including nonsubscribers.[12] The OTC providers are, formally, subagents operating on behalf of licensed FIs. In practice, they operate with wide autonomy and include well-established OTC companies that operate throughout WAEMU. The OTC providers are significant for a number of reasons. First, they extend access to payments and money transfer services to customers who may not have digital accounts (or may not use them). The providers are not e-money issuers or payment services companies, and their services are perceived as relatively cheap. On the other hand, OTC services are limited to person-to-person (P2P) fund transfers and some bill payments, and so are not as convenient as having one's own mobile money account. Second, firms such as Wari and Joni Joni provide OTC services on a large (regional) scale, using wide retail networks that potentially give them a very strong competitive base to offer agent

9 These include account opening, certain teller and ATM services, account statements and others. *Instruction n° 04/06/2014 relative aux services bancaires gratuits offerts par les établissements bancaires de l'UEMOA à leur clientèle.* In the instruction, BCEAO simply listed the services without defining them. Reportedly, as a result, some banks have changed the names of the relevant services and charge for them.

10 This strategy has been approved but not yet implemented. The relevant action plan is available at http://microfinance.tresor.gouv.ci/m/wp-content/uploads/2016/download/autres/Strategie-plan-d-actions.pdf. Côte d'Ivoire has also improved the tax treatment of DFS. Fiscal legislation in 2015 shifted the value-added tax (VAT) on money transfers from a system of differentiated rates based on the types of institutions involved to a uniform rate of 18 percent. The base for this tax appears to be the fee or commission, not the transfer amount.

11 We use "OTC provider" or "OTC company" to refer to the operator who interacts with customers in delivering fund transfer services, even though this operator is legally a subagent of an FI.

12 These agents use an online platform linked to a bank account. It is important to distinguish this OTC model from those prevalent in other regions and countries, where the same terminology refers to a different arrangement such as where the client's own account is used.

banking and e-money issuance. Wari, a regional OTC services provider, competes with the MNO-affiliated issuers in Côte d'Ivoire and has launched a Visa card in partnership with a bank linked to the regional card switch.

2.2 Market infrastructure

In terms of DFS-related infrastructure, Côte d'Ivoire is modernizing infrastructures that relate to DFS and addressing deficits that accumulated during its period of conflict. The government is pursuing a strategy aimed at closing the digital divide. A key component is the creation of a 7,000 km-fiber-optic "backbone" for digital communication, of which about one-third has been laid. The expectation is that this will attract private investment in digital communication and information systems. In addition, the telecom authority has moved to simplify licensing, while government has adopted a policy of moving administrative services online.

Côte d'Ivoire has also made progress on the digitization of government payments, in contrast to many of the other WAEMU countries (Koné 2016). All secondary school registration fees in Côte d'Ivoire have been paid via mobile money since 2014, and this is leading other public agencies to digitize incoming payments as well. This digitization should encourage DFS development as it has elsewhere.

Until recently, the national ID system had been a hindrance to DFS outreach. It is now reaching the majority of the population. A national ID database is being developed and should facilitate the move to fully digital account access. In parallel, the telecom regulator in Côte d'Ivoire has been tasked with identifying all SIM card subscribers; this is expected to ease digital security concerns.

Agent networks for FIs have been constrained, in large part by policy factors, but MNOs have growing networks that are increasingly involved in DFS. (Orange alone has about 10 times the number of service points as the banking system.) Agents are still fairly concentrated in urban areas and do not always have sufficient access to technical support and liquidity.

Limited interoperability between payment systems, cards, and mobile wallets is still an important problem. This issue, which has both technical and policy dimensions, has been under discussion. A key part of the eventual solution is now in place with the establishment of a regional payments switch, GIM-UEMOA (*Groupement interbancaire monétique de l'UEMOA*) (discussed in the next section).

3. E-MONEY AND PAYMENTS

The cornerstone of many DFS frameworks is the legal and regulatory regime that governs e-money. This comprises rules on e-commerce, authorization and oversight of e-money providers, and allocation of activities to distinct service and regulatory fields, such as banking and payment systems.

3.1 E-money: Regulatory definition and treatment

The key instrument here is the 2015 BCEAO instruction,[13] which updates the 2006 rules on e-money. This instruction (art. 3) governs all e-money transactions, including those carried out by card, internet, and telephone. (An overview of key e-money rules is given in Table 1.) E-money is defined (art. 1.16) as:

- A monetary value, representing a liability for the issuer, stored in electronic (including magnetic) form.
- Issued without delay against funds provided in at least an equal amount.
- Accepted as a means of payment by third parties (both individuals and companies).[14]

This definition appears to conform to good international practice as represented, for example, by the European Union's E-Money Directive (2009/110/EC). Importantly, the definition in the instruction enables issuers to accept funds from the public for purposes of e-money issuance without (simply for that reason) having to obtain a deposit-taking license.

The instruction allows for a few different kinds of issuers. The banking and microfinance laws[15] provide for the following categories of FIs: (*i*) commercial banks; (*ii*) payment services companies,[16] a category of nonbank financial institutions (NBFIs) (*établissements financiers à caractère bancaire*); and (*iii*) MFIs. Under the e-money instruction, all three of these types of institutions are permitted to issue e-money with a few preconditions. However, the MFIs face a (potentially) major limitation here with respect to e-money and related activities other than savings and credit. Under the microfinance regulation, an MFI's revenue from nonsavings/credit services is strictly capped (at 5 percent of the institution's "risks"), unless permission is obtained from the Minister of Finances with consent from BCEAO.[17]

Banks and payment services companies must notify BCEAO (two months) in advance of any deployment, while MFIs must get prior authorization[18] from the Minister of Finances after BCEAO

13 Instruction N°008-05-2015 *régissant les conditions et modalités d'exercice des activités des émetteurs de monnaie électronique dans les Etats membres de l'Union Monétaire Ouest Africaine* (UMOA).

14 The full definition is as follows: "*une valeur monétaire représentant une créance sur l'établissement émetteur qui est stockée sous forme électronique, y compris magnétique, émise sans délai contre la remise de fonds d'un montant qui n'est pas inférieur à la valeur monétaire émise, et acceptée comme moyen de paiement par des personnes physiques ou morales autres que l'établissement émetteur.*"

15 *Loi-cadre portant réglementation bancaire; Loi portant réglementation des systèmes financiers décentralisés*; *Instruction n° 011-12/2010/RB relative au classement, aux opérations et à la forme juridique des établissements financiers à caractère bancaire; Décret d'application de la loi portant réglementation des systèmes financiers décentralisés*.

16 *Etablissements financiers de paiement.*

17 Annexe vi-Limitation des opérations autres que les activités d'épargne et de crédit (article 36, *Loi portant réglementation des SFD*). "Risks" here refers to provisions against all risk assets. BCEAO points out that this rule has a prudential rationale, i.e., to help ensure that the core MFI business is strongly established before other activities are undertaken. Discussions are under way on adjustments to the MFI regulations, including this provision.

18 E-money instruction, arts. 8–14. We distinguish "authorization" (*autorisation*) from "license" (*agrément*). An authorization is an approval by the central bank (technically, per the MFI law, the Minister of Finances acting on the advice of BCEAO) for an FI to issue e-money, an activity that the institution is permitted to carry out with prior approval. A license is a permit to issue e-money obtained by a non-FI, and this requires more thorough scrutiny by the central bank.

TABLE 1. WAEMU rules on e-money: Key features

Regulatory features	WAEMU provisions
Definition of e-money	E-money is defined as (*i*) a monetary value, representing a liability for the issuer, stored in electronic (including magnetic) form; (*ii*) issued without delay against funds provided in at least an equal amount; and (*iii*) accepted as a means of payment by third parties (both individuals and companies). It does not include closed-loop mechanisms.
Who may be an e-money issuer	E-money issuers can be banks, payments companies (category of NBFI), MFIs, and authorized nonfinancial companies (including affiliate companies set up by MNOs).
Prudential requirements	Banks, payments companies, and MFIs must meet ongoing prudential requirements per their licenses and BCEAO supervision. Non-FI issuers (EMEs) must meet an initial paid-up capital threshold of 300 million FCFA (~US$500,000). MFIs meet this requirement if their own funds and total client deposits on their books, combined, meet the threshold. EMEs must, at all times, have equity of at least 3% of outstanding e-money issued (and at least equal to their minimum share capital requirement).
Reporting requirements	Monthly reports on e-money outstanding and e-money float balances in trust accounts. Quarterly reports on capital ratios against e-money outstanding, balances in trust accounts, balance sheet, e-money account volume and activity, total numbers of agents and service points, figures on mobile money and card transactions, risk indicators for new products, and fraudulent transactions. Annual audited financial reports.
Fund safeguarding requirements	Funds converted to e-money to be placed in bank or MFI accounts set up for this purpose—and separately identified in the accounts of the issuer and depositary institution. The funds must be reconciled daily against e-money issued, and settlement must be carried out by means of a payments system approved by BCEAO. E-money float must always be at least equal e-money outstanding. At least 75% of the value of all e-money in circulation must be kept in sight/demand deposits. Beyond this, funds may alternatively be placed in time deposits, T-bills, or corporate securities (of listed companies). No trust account structure required; applicability of deposit guarantee is unclear.
Rules on float account	E-money float is not to be exploited for the account of the issuer. No interest may be paid on the float. Issuers may be required to repay funds at any time at the par value of the outstanding e-money balance. Otherwise, reimbursement terms are set by contract.

consent. All must meet generally applicable standards and comply with the e-money rules. We refer to these FIs, who hold existing BCEAO licenses along with e-money authorizations, as "FI issuers."

Nonfinancial companies may also issue e-money after obtaining a license. These issuers are called *Etablissements de Monnaie Electronique* (EMEs or "non-FI issuers"). They must meet separate standards on corporate governance and related matters (e.g., fit-and-proper standards, internal controls) to obtain a license.[19] These EME companies must be solely dedicated to e-money issuance, (i.e., providing payment, transfer, and cash-in/out services [*distribution de monnaie électronique*]). They cannot provide savings or credit services. EMEs can own shares only in other entities involved in e-money issuance.

As mentioned, some MNOs are in the process of setting up e-money subsidiaries to use this EME license—or have done so already[20]—in preference to partnering with (or acquiring) a bank. The e-money instruction (art. 4) limits issuers' partnership arrangements. Issuers may enter such agreements only with technical operators who restrict their activities to the "technical treatment" of e-money (and who are not responsible for issuing e-money). This provision appears designed to clarify the roles and responsibilities between the e-money issuers and the technical operators, and to encourage MNOs to focus on providing the technology platform. Thus, an MNO may be the technical operator for either (*i*) a partner bank (or other partner FI) or (*ii*) an EME (non-FI) that the MNO partners with or establishes as an affiliate.

The two groups (FI issuers and EMEs), considered together, are called *établissements émetteurs*, and can simply be referred to as "issuers." Thus, the following institutions, if they meet their respective BCEAO authorization or notice requirements, may issue e-money: banks, payment services companies, MFIs, and EMEs (non-FI issuers). The following sections address the scope, limitations, and requirements in connection to this.

3.2 Protection of funds

Issuers must promptly deposit funds received from e-money clients in accounts specifically for this purpose at one or more banks or MFIs. This e-money float is to be separately identified in the accounts of the issuer and depositary institution—and the total held by each issuer must be at least equal to the amount of e-money outstanding at all times. The placement of these funds is prescribed. An issuer must place at least 75 percent of the value of all its e-money in circulation in sight/demand deposits; beyond this threshold, time deposits, T-bills, and corporate securities (of listed companies) are acceptable. The funds received must be reconciled daily (by the issuer and the depositary institution) against e-money issued, and settlement must be carried out by means of a payments system approved by BCEAO.[21]

The instruction prohibits issuers from issuing e-money as credit and from paying interest on e-money float. But this does not prevent banks and MFIs from linking a client's e-money account to her/his other accounts—for example, credit or savings.[22] Issuers are responsible

19 These standards are not applied to FI issuers for purposes of e-money authorization because their existing BCEAO licenses require them to meet at least equivalent standards.

20 I.e., Orange and MTN in Côte d'Ivoire.

21 E-money instruction, arts. 32–35. Other placements of e-money float are not permitted: "*Ils ne doivent pas être utilisés au financement des besoins de l'exploitation de l'établissement émetteur*" (art. 32).

22 E-money instruction, art. 5: *"Les établissements émetteurs ne sont pas autorisés à consentir . . . des services de crédit à leur clientèle, ni à payer des intérêts sur les fonds perçus en contrepartie . . . .Toutefois, les fonds provenant d'un crédit octroyé à un client par une banque ou un SFD peuvent être utilisés pour émettre de la monnaie électronique."*

for ensuring prompt reimbursement of unused funds upon the client's demand, according to the terms of the e-money contract—but in any case within three business days.[23] In contrast to practice elsewhere (e.g., Kenya, Rwanda), the BCEAO e-money instruction does not require placement of the funds in a specially structured account (trust or escrow) to isolate them from claims on the issuer. ***In case of the issuer's bankruptcy, for example, it appears that the issuer's creditors would be able to assert claims against the float funds.***

Beyond this, the protection of e-money float depends on whether deposits are insured. Côte d'Ivoire has adopted a deposit guarantee scheme (based on regional standards) that covers individual and business accounts, but not wholesale deposits by banks, MFIs, or investment companies.[24] This scheme is not yet in operation, nor is it fully clear how it would treat e-money float. In principle, bank deposits by EMEs (including the required proportion of e-money float placed in sight deposits) would be covered by the guarantee.[25] But it is not yet clear how e-money float deposits would be treated in practice. Presumably, e-money float received and held by the same FI issuer could be covered by the guarantee, but not funds placed elsewhere (including another bank or MFI) by that issuer. In any event, large pooled deposits would quickly exceed the deposit guarantee ceiling (per account). ***The DFS market would be strengthened if policy makers in Côte d'Ivoire (and across WAEMU) could clarify or rationalize the application of deposit guarantees to e-money float.***

The e-money instruction (art. 31) imposes quantitative limits on e-money holdings per client: a maximum e-money balance with a single issuer of 2 million FCFA (~US$3,400) and a maximum of 10 million FCFA (~US$17,000) in recharges (topping-up of balance) per month across all institutions.[26] These ceilings apply to customers and issuers, but not to e-money agents or payees (merchants). (The agents and merchants are not responsible for customer compliance with the ceilings.) The instruction also has provisions on customer identification (see Section 5).

3.3 Issuers: Regulatory requirements

As a condition for authorization, EMEs must meet an initial paid-up capital threshold of 300 million FCFA (~US$500,000) (e-money instruction, art. 11). MFIs may be authorized to issue e-money if the sum of their own funds and the total amount of customer deposits in their books reach this minimum threshold of 300 million FCFA at the end of the financial year preceding the date of the application for authorization. The MFIs, banks, and payments companies must meet ongoing prudential requirements per their licenses and BCEAO supervision. EMEs must, at all times, have equity of at least 3 percent of outstanding e-money issued (and at least equal to their minimum share capital requirement). BCEAO expressly

23 Clients may obtain reimbursement from an agent of the issuer, but responsibility for timely performance rests with the issuer (art. 35). The issuer's contract with the client may place conditions on reimbursement, consistent with the instruction. This could in principle (and within reason) require clients to approach specially designated agent(s) for this purpose.

24 *Statuts du fonds de garantie des dépôts dans l'Union Monétaire Ouest Africaine (UMOA) 2014,* art. 22.

25 EMEs are treated as ordinary businesses depositing money, while FIs and FI-issuers are responsible under their licenses for bearing the risks of any fund placements—and thus are not covered by the guarantee. However, since all these deposits are more like aggregated individual deposits than large-investor deposits, they fit the rationale of the deposit guarantee.

26 E-money instruction, art. 31. Unlike e-money regulations elsewhere, the BCEAO instruction refers not to transactions but to holdings (*les avoirs*) and recharges of holdings (*rechargements*). This corresponds most closely to a maximum balance (at any time) and a ceiling on cumulative monthly e-money purchases (hence also expenditures/sales).

reserves the authority to increase the required capital for any EME based on its risk assessment.

Whereas banks must simply notify BCEAO, MFIs must apply for an e-money authorization—and thus meet the capital requirement. This could, in some cases, require them to increase their capital. Under the law on MFIs and subsidiary regulations,[27] there is no fixed minimum capital for MFIs—rather, a capitalization formula in which shareholders' equity or *fonds propres net* exceeds assets by 15 percent. To become an e-money issuer, an MFI must have a minimum of 300 million FCFA in *fonds propres net* combined with total client deposits. Thus, minimum capital and capital ratios vary from one MFI to another, and may be more or less than the e-money license requirement.[28] Also, as in the case of EMEs, BCEAO may decide to call for increased capital based on its assessment of risk. This last point fits with the perception that BCEAO has been quite strict in considering e-money license applications, especially from MFIs, taking into account factors such as overall resources, information systems, and organizational vision.

Authorization and licensing applications require documents such as business plans, financial projections, risk management approach, and technical systems architecture (e-money instruction, Annex I). All issuers are subject to prudential supervision by BCEAO, including inspection and sanctions, and reporting requirements (monthly and quarterly, arts. 36–37). Issuers are further required to provide for secure and reliable e-money platforms, guarantee the integrity and confidentiality of information used in their services, and establish satisfactory internal control and risk management systems.[29]

3.4 E-commerce, e-signature

E-money (and DFS, generally) depends on the framework for e-transactions. The critical component here is the certification of digital documents (with e-signatures) that have replaced paper documents. There is both national and regional legislation in this area, including the 2002 WAEMU payments regulation[30] and more recently (2013–2014) the Ivoirian legislation on e-transactions and e-signatures.[31]

The 2002 WAEMU regulation applies by virtue of the Union's (and BCEAO's) predominant authority over financial services. Under the regulation (arts. 17–30), an e-signature certified by a qualified, approved entity has the same validity as a physical signature (for purposes of payments)—and the certificate need not be presented when the signature is used, unless its authenticity is questioned.

---

27 *Loi portant réglementation des systèmes financiers décentralisés; Instruction n° 010-08-2010 relative aux règles prudentielles applicables aux systèmes financiers décentralisés des Etats membres de l'Union Monétaire Ouest Africaine (UMOA); Annexe viii: norme de capitalisation; Instruction n° 005-06-2010 déterminant les éléments constitutifs du dossier de demande d'agrément des systèmes financiers décentralisés dans les états membres de l'Union Monétaire Ouest Africaine (UMOA),* art. 4.

28 At the time the current microfinance law was enacted in 2008, the sector followed a mutualist model of financial cooperatives, federations, and apexes. Minimum capital and capital adequacy were not given a fixed definition across the sector (as in a number other savings and credit cooperative worldwide). The new law and regulations inserted prudential rules aimed at shoring up the cooperatives and accommodating new MFIs based on a corporate model. For the new corporate MFIs, share capital must be fully paid up before approval of the institution's license (and must be fully subscribed and at least 25 percent paid up before the license application). All MFIs must meet capitalization norms aimed at ensuring solvency. The capitalization formula requires the MFI's own funds or shareholders' capital (*fonds propres net*), broadly defined to include forms of lower-tier capital such as subsidized capital and subordinated debt, to exceed total assets by at least 15 percent.

29 These arrangements are stated explicitly for EMEs. For FI issuers, they are mentioned in the context of their duty to comply with BCEAO prudential requirements (e-money instruction arts. 16, 25).

30 R*èglement N° 15/2002/CM/UEMOA relatif aux systèmes de paiement dans les états membres de l'Union Economique et Monétaire Ouest Africaine (UEMOA).*

31 *Loi no. 2013-546 du 30 juillet 2013 relative aux transactions électroniques; Décret no.2014-106 du 12 mars 2014 fixant les conditions d'établissement et de conservation de l'écrit et de la signature sous forme électronique.*

Côte d'Ivoire's e-transactions law (art. 50) places e-commerce under the jurisdiction of the national telecoms regulator (*Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire* or ARTCI). The law includes provisions on advertising, offer and acceptance, contracts, transparency of prices, and ID of the seller/provider—its definition of e-commerce clearly includes DFS. E-documents (and e-signatures) that meet security standards have the same legal validity as paper copies (arts. 23–35).[32]

The Ivoirian legislation contains provisions parallel to those of the 2002 WAEMU payments regulation on the form, validity, and certification of e-signatures. The 2013 law deals with e-transaction security (arts. 36–39), including e-signatures. The 2014 decree imposes security requirements on e-signatures, for example, exclusive control by the signatory and protection from manipulation and unauthorized use (arts. 3–7). An e-signature cannot be accepted unless it is secured by a qualified e-certificate (arts. 8–12) delivered by ARTCI or an approved provider. The contents of these certificates are defined along with procedures and requirements for approval of the certificate provider.[33]

Thus, regional and national regulations each provide in principle for transactions to be carried out and signatures to be made effective entirely by digital means, once a certified e-signature is in place. In both instances, procedures are outlined for signature certification and for the registration of certification services providers.[34]

In practice, however, it is reported that fully electronic processes for account opening are not possible in Côte d'Ivoire because paper certificates are required to back e-signatures. This complicates the opening of digital accounts, and (prospectively) the conclusion of digital credit agreements. According to ARTCI, individuals must apply for e-certificates directly (i.e., in person or through an authorized representative). It is possible that ARTCI-approved certificates do not meet the requirements of the 2002 payments regulation. ***Such inconsistencies would need to be resolved by either interagency agreement or by another appropriate intervention.***

According to BCEAO, work is underway to craft revisions to the 2002 payments regulation, including removal of the requirement to retain physical signatures (art. 19). Further, regionwide certification is expected to be provided by *Système Ouest Africain d'Accréditation* (SOAC)—a body established in 2005, but not yet operational.

3.5 Payments

The e-money rules were introduced into a landscape already shaped by earlier legislation on payment systems. The utility of e-money as a means of payment raises the question of how it fits with existing payments systems. The 2002 WAEMU payment regulation sets the ground rules here. The regulation puts BCEAO in charge of supervising all payment systems (including their security and smooth functioning), and it authorizes banks, MFIs, the Post, and the Treasury to provide payment services.[35] The 2010 BCEAO instruction classifying non-bank institutions includes a specialized

32 E-commerce documents are to be archived for 10 years (unless there is a provision calling for a shorter period [art. 40]).

33 These provisions are broadly consistent with the UNCITRAL Model Law on Electronic Signatures, but they lack equivalent detail, which could be developed in Côte d'Ivoire in the course of implementation. Additional security for e-data is provided by *Loi no. 2013-451 du 19 juin 2013 relative à la lutte contre la cybercriminalité.*

34 As BCEAO points out, regional-level legislation (in fields encompassed by regional jurisdiction) prevails over measures adopted at the national level, and thus in principle there is no conflict. In practice, however, there are some inconsistencies.

35 BCEAO's supervisory role here was further defined in *Instruction n°127-07-08 du 9 juillet 2008 fixant les modalités de mise en oeuvre de la surveillance par la BCEAO des systèmes de paiement dans les Etats membres de l'UEMOA.*

BOX 2. WAEMU Payment and Settlement Systems[a]

The main systems for digital transfers and settlements in WAEMU are GIM-UEMOA, SICA-UEMOA, and STAR-UEMOA. GIM-UEMOA is a unique ATM and POS switch for card payments across UEMOA. SICA-UEMOA is the automated retail payments exchange and settlement system. It handles transfers of up to 50 million FCFA (US$85,000). Settlement of payments through SICA-UEMOA and GIM-UEMOA are linked to a deferred settlement arrangement under STAR-UEMOA, the wholesale payments system that handles amounts above the SICA-UEMOA limit. SICA-UEMOA comprises nine settlement systems (a regional system and one for each WAEMU member). STAR-UEMOA essentially handles interbank transfers, settlement of securities transactions (for liquidity purposes), and others in real time, along with (delayed) wholesale settlement for SICA-UEMOA and GIM-UEMOA. BCEAO supervises STAR-UEMOA and SICA-UEMOA, and it owns a majority share in GIM-UEMOA. Membership in these payment systems is limited to BCEAO, banks, NBFIs (STAR-UEMOA), and treasury and postal authorities (SICA-UEMOA). (Per-transaction commissions are set at 100 FCFA for SICA-UEMOA and 150–420 FCFA for STAR-UEMOA, depending on timing and volume.)

a. World Bank, *Diagnostic des paiements de détail et stratégie pour développer leur utilisation dans l'UEMOA*, draft report, October 2014; BCEAO website.

category of companies authorized to provide payment services. Other NBFIs may also provide such services with prior authorization from BCEAO.[36]

Payment methods covered by the 2002 regulation include (in addition to negotiable instruments) e-transfers, bank cards (ATM and payment cards), and prepaid cards.[37] The regulation requires participants in payment systems to abide by the rules set by each system, and it sets general standards for reliability, security, and enforcement of e-transactions (later strengthened in Côte d'Ivoire by the 2013 e-commerce legislation). Payment services offered by the Post also come within the purview of BCEAO, under the 2002 payments regulation. Côte d'Ivoire's postal legislation[38] provides for issuance of money orders (*mandats*)—fund transfers that were traditionally sent by mail but are increasingly electronic. In addition, the Post is authorized to serve as an agent for e-money services (see Section 4). It has sought to market its products in partnership with commercial entities, for example, teaming with Western Union on international transfers and with BHCI bank on a prepaid card and e-wallet smartphone app.

The payments regulation does not differentiate between wholesale and retail payments. The bank-based payment systems account for most large-volume and bulk payments (as well as much of the retail payments traffic). In practice, the e-money system is focused on small-value, low-volume transactions. Payments made by means of e-money are covered by the regional payments legislation, and so are subject to the rules of the relevant payment systems. (See Box 2.)

36 *Instruction N° 011-12/2010/RB,* arts. 8, 9.

37 A prepaid card is (somewhat confusingly) designated in the regulation as a *porte-monnaie électronique.*

38 *Loi no. 2013-702 du 10 octobre 2013 portant Code des Postes.*

We could describe the payments and e-money systems in WAEMU as a series of loops that are largely closed and not interoperable. BCEAO is responsible for supervising them and ensuring security, but there has yet to be a strong push to rationalize this payments ecosystem so that its different participants can play together on the same level playing field. Recent studies have advocated such a reform to harmonize the various systems (World Bank 2014). This is discussed further in Section 7.

4. USE OF AGENTS

Widespread access to agents that operate under appropriate safeguards is also critical to DFS, and to financial inclusion, generally. For simplicity, we use the term "agent" to refer to a third party acting as a primary, retail-level, or subcontracted representative or distributor for DFS or banking services. Authorizing the use of agents opens up the possibility of broad distribution networks. The regulatory framework in WAEMU enables financial services providers to use agents for e-money and rapid (OTC) fund transfers, but it is more restrictive with respect to agent banking. (See Table 2A for a synopsis of key rules on the use of agents.) The scope for use of agents by different organizations in this field is approximately as follows:

- Permitted to use primary agents (distributors) and retail agents (subagents)[39] for *e-money services*, under the 2015 e-money instruction: Banks, payments companies, MFIs, and EMEs (including MNOs).
- Permitted to use retail agents (subagents)[40] for *OTC transfers* under the 2015 rapid fund transfers regulation: Banks, payments companies and other NBFIs, and MFIs.
- Not legally empowered but may be permitted by BCEAO on an exceptional basis to use agents for *microfinance* services, under the MFI law and recent BCEAO practice: MFIs.[41]
- Permitted to use *banking* agents (intermediaries/IOBs)[42] under restrictive conditions defined in a 2010 BCEAO instruction: Banks.

4.1 E-money

The e-money instruction (arts. 2, 17) provides for a two-tier system of primary agents and subagents. Those permitted to serve as primary agents are retailers and other businesses (registered companies or individuals) as well as MFIs, the Post, and other NBFIs. These agents may then outsource to subagents, who must be registered businesses (including individuals and companies). The qualifications of agents and subagents are not specified in the instruction, beyond those just mentioned.[43]

As for services that can be outsourced to agents, these come under the heading of marketing and supply of services related to e-money (e-money instruction, art. 17), and include signing up clients to e-money accounts (i.e., processing applications on behalf of the issuer[44]), cash-in and cash-out, and payment services.[45] Exclusive agency agreements (i.e., those that require an agent to serve a single issuer exclusively) are prohibited.

The issuer (principal) remains legally responsible to its clients and third parties for all of the services contracted out to its primary agents (e-money instruction, arts. 2, 17–18, 25). Among the duties of

39 Called *distributeurs* and *sous-distributeurs*.

40 Called *sous-agents*.

41 BCEAO reports that it received a request to this effect from Microcred Côte d'Ivoire in 2016, but that it is still considering the matter and has not issued a formal decision to authorize or prohibit agents in this case.

42 This is "agent banking" or providing core banking services such as savings and credit through an agent. Regulations on e-money and rapid transfers permit banks to use ordinary (not IOB) agents for the limited purpose of providing those particular services.

43 As noted in Section 3, partners are in a different category. They may only supply or operate technology solutions, and are otherwise not permitted to participate in e-money issuance (e-money instruction, art. 4).

44 "*La souscription des contrats d'utilisation* [user agreements] *avec la clientèle*."

45 Also, the payments regulation of 2002 (art. 1) supports the use of intermediaries in payments systems.

TABLE 2. Rules on agents in DFS

Regulatory features	WAEMU provisions
Who may use agents, for what purpose	Banks, payments companies, MFIs, and EMEs (including MNOs) permitted to use agents and subagents for e-money services. Banks and MFIs are permitted to use (sub-) agents for rapid fund transfers. Permissibility of using agents for ordinary banking services is limited for banks, and unclear for MFIs. Banks may use agents (IOBs) under restrictive conditions. BCEAO has in effect allowed an MFI in one case to use agents for microfinance services (regulation does not expressly permit).
Who may be an agent: eligibility	E-money agents may be MFIs, NBFIs (including the Post), and registered businesses (individuals or firms)—the last group may also be subagents for e-money and rapid transfer. Qualifications of agents and subagents are not spelled out in DFS legislation. Any fit-and-proper standards would be imposed by the agent's charter or registration.
Liability of DFS provider for agents	E-money issuers are legally responsible to their clients and third parties for their agents. Issuers' responsibilities includes the reliability, security, confidentiality, and traceability of transactions conducted on their behalf by the agents. The same is true for rapid transfer services provided by agents.
Risk assessment procedures for provider to use agent channel	E-money issuers must ensure that their agents have appropriate internal control, accounting, and risk management procedures and manuals. Agents must have sufficient liquidity to meet the needs of e-money holders/clients, and must ensure the traceability of transactions. All issuers must send BCEAO descriptions of the risk management arrangements they have in place—in particular, those dealing with agent liquidity. For rapid transfer, the agency agreement must specify that the agent acts under the comprehensive responsibility of the principal, though due diligence procedures are not spelled out. The principals using agents for transfer services must be banks or MFIs.
Permitted and prohibited activities for banking and non-banking agents	E-money services that can be outsourced to agents include the signing of user agreements with clients, cash-in and cash-out, and payment services. Transfer (sub-) agents are limited to sending and receiving transfers and related cash handling, but may not carry out any other banking function such as deposit collection (except if the agent is an MFI). Banking agents (IOBs) provide core banking services under restrictive conditions, and under the banks' supervision and liability.
General reporting requirements to the supervisor	E-money issuers must report to BCEAO the current list of agents, and the risk mitigation measures in place in its agent network, including governance and liquidity risks. Transfer agents' principal institutions must send BCEAO annual updated lists of agents, a copy of the model agency contract being used, and monthly reports on transfer operations by their agents. Banking agents (IOBs) must submit periodic reports to BCEAO on the nature and volume of their business.
Exclusivity	Contracts binding an e-money agent exclusively to a single issuer are prohibited. The same rule applies to transfer subagents and their principals. No such rule for IOBs but an IOB can operate for several banks.

the agent, for which the issuer is ultimately responsible, are the following:

- Conducting the necessary due diligence on clients and providing for the security of all its transactions.[46]
- Ensuring the confidentiality and traceability of the transactions they handle.
- Having sufficient liquidity to meet the needs of e-money holders/clients (arts. 17–18, 25).
- Informing the public (by posting and other means) of the identity and contacts of the issuers they represent.

Agents are also required to report activities raising suspicion of money laundering to the issuer, who is responsible for any further steps in this regard (art. 26, see Section 5).

Thus, issuers bear primary responsibility for supervising their agent networks, with BCEAO playing a higher-level oversight and inspection role. All issuers must send BCEAO updated lists of their agents on a regular basis (as part of regular monthly and quarterly reporting), along with descriptions of the risk management arrangements they have in place—particularly those dealing with agent liquidity. There is no requirement of prior approval by the regulator. However, BCEAO may check the legal compliance of agency arrangements *ex post.*

A few additional rules apply to the EMEs—which do not, unlike the other issuers, have an existing financial services license. The e-money rules (art. 37) grant BCEAO the authority to inspect EMEs along with their e-money agents and technical services providers—bringing in other regulatory authorities as needed. Further, EMEs are expressly required to have appropriate internal control, accounting, and risk management procedures and manuals—and to ensure that their agents do as well.[47]

4.2 Transfers

In addition, a BCEAO instruction[48] authorizes banks, NBFIs, and MFIs to provide rapid fund transfers—i.e., over-the-counter (OTC) transactions—by means of retail agents (*sous-agents*). The "OTC" designation is used in a variety of ways across different markets. One definition of transactions as OTC is simply that "at least one end of the transaction is conducted without involving the wallet of the user—either the sender or the receiver."[49] The BCEAO instruction defines the relevant transactions as real-time transfers (within UEMOA[50]) performed OTC at an authorized provider or agent, and not involving any bank or e-money account (of either the sender or recipient).

The instruction sets a number of conditions for use of rapid transfer agents. The agents (OTC providers) act under the comprehensive responsibility of the principal (FI) and for the principal's account. Agents have a role in customer due diligence similar to that of e-money

46 Primary agents execute contracts with clients on behalf of the principal. Subagents, in turn, sign contracts on behalf of the primary agents who hire them, and under the overall responsibility of the issuer.

47 These rules appear aimed at bringing EMEs under the same oversight as FIs acting as issuers.

48 *Instruction N° 013–11–2015 relative aux modalités d'exercice de l'activité de transfert rapide d'argent en qualité de sous-agent au sein de l'Union Monétaire Ouest Africaine.*

49 "OTC transactions . . . come in many forms in different markets—from the direct deposit by the agent into the end-user's wallet in Kenya to the transfer of money from one agent to another agent, with or without identification, in Pakistan and Bangladesh respectively" (Wright 2014).

50 Movement of funds to countries outside the region is restricted to institutions such as the Post, change bureaus, and others approved under *Règlement R09/2010/CM/UEMOA du 1er octobre 2010 relatif aux relations financières extérieures des Etats membres de l'UEMOA*, art. 2.

agents. The principal institution is primarily responsible for ensuring that its agents comply with the transfer rules, but BCEAO has discretion to inspect the agents directly. Agents are not subject to prior approval, but their principal institutions must send BCEAO (and the Banking Commission and Ministry of Finance) annual updated lists of agents, a copy of the model agency contract being used, and monthly reports on transfer operations by their agents. Exclusive agencies are prohibited, as in the case of e-money agents. Lastly, rapid transfer agents are not allowed to collect funds for reasons other than OTC transfer (e.g., deposits)—unless the agent is an MFI.

FIs and EMEs, among others, have expressed concern about low-cost competition from OTC providers and the relatively light regulation to which the latter are subject. However, given the lower risk profile of transfers as compared to other forms of DFS, such as e-money, a lesser regulatory burden and lower costs are to be expected. The OTC framework appears to make a valuable alternative available to DFS customers.

4.3 Agent banking

Beyond e-money and OTC transfers, the scope for using agents is less clear. Agent banking has proven difficult. The rules are highly restrictive for banks, and there is no explicit framework for MFIs. Banks are authorized to use *Intermédiaires en Opérations de Banque* (IOB), a type of agent, by the banking law (art. 105) and a 2010 BCEAO instruction.[51] This instruction requires each prospective IOB to obtain separate, prior approval from the Ministry of Finance on the advice of BCEAO. Each IOB is subject to fit-and-proper standards, a required financial guarantee (by a principal bank[52]), and regular reporting. Banks are responsible for direct supervision of IOBs and for maintaining an updated list of IOBs with the central bank. Technical, operational, and governance standards for IOBs are not spelled out in the BCEAO instruction. (They are presumably defined in the agency agreement with the principal bank and the terms of approval by the Ministry and central bank.)

World Bank (2016) concludes that this structure is not at all well-designed to support agent banking in the DFS context, especially since it makes the establishment of large agent networks costly and difficult. ***Indeed, the IOB model (originally derived from French commercial law) did not come into being as an instrument for expanding financial inclusion. It is a business niche for a "middle man" (intermédiaire) operating within the traditional banking sector and on its (her/his) own account—comparable to an insurance agency. The procedures involved in setting up an IOB, including the requirement of a guarantee, encourage the banks to have fewer (more financially solid) IOBs rather more small outlets.*** Thus, from the introduction of the rules in 2010 until early 2016, only five IOBs were approved and registered by BCEAO in the region. Further, in contrast to the e-money instruction, the IOB instruction is silent on whether IOBs can contract out functions to subagents. In the context, this silence is to be understood as a negative. IOBs, then, cannot subcontract, but in practice they do have multiple outlets (branches and satellite offices).[53]

51 *Instruction N° 015-12/2010/RB fixant les conditions d'exercice des activités d'intermédiaires en opérations de banque*.

52 E.g., for an IOB handling bank deposits, the required guarantee (or insurance policy) is approximately US$26,000.

53 Branches and satellite offices are captured in the term *agence* used several times in the banking law (e.g., arts. 15, 25)—i.e., they are not legal agents but service points staffed by the bank.

For MFIs, the issue of providing credit and savings services through agents is not addressed directly. The microfinance law (art. 36) is silent on the use of agents but recognizes that the MFIs have discretion to enter arrangements to better serve their clients. Conditions and standards for MFI agent services are not defined in the legislation. In practice, BCEAO has authority to permit MFIs to use agents for core financial services on a case-by-case basis. The central bank recently allowed an MFI (Microcred) to launch an agent banking pilot in Senegal.[54]

54 As noted, BCEAO has not made a formal determination, nor has it halted the pilot. It is not clear what conditions apply to agents operating under this pilot. Microcred's agents network concept is briefly described at http://www.microcredgroup.com/fr/solutions/innovation-et-technologie/b/60-87-

5. CUSTOMER IDENTIFICATION

Expanding access to DFS requires secure methods of identifying clients. A proportionate approach that calibrates such safeguards based on risk is also needed. The issue of identification arises particularly in the context of policies on AML/CFT (see Box 3).

Anti-money laundering legislation poses the challenge of balancing safety against financial inclusion in the design of KYC rules and procedures. In light of this, the policies and systems for ID documentation and then the KYC requirements applied to DFS customers are addressed in the following.

5.1 Identity documentation

In the financial system, BCEAO regulations determine when ID must be presented and what additional information is to be collected for KYC purposes. The system of official ID documentation itself, by contrast, is a matter of national policy. In Côte d'Ivoire, recent efforts by the government have resulted in some 70 percent of the Ivoirian population (as of mid-2016) having official IDs. Further, the National Office for Identification is in the process of establishing a comprehensive digital identifier system as part of an overall reform of civil status and identity records.[55]

The Ivoirian telecoms regulator, ARTCI, sets the rules for identifying customers who wish to obtain SIM cards, internet subscriptions, and other forms of digital access. Starting in 2009, ARTCI sought to identify all users of prepaid SIM cards

BOX 3. AML/CFT legislation in WAEMU[a]

A 2015 WAEMU directive provides anti-money laundering safeguards for the financial sector and for a wide range of actors involved in relevant activities. The list of entities covered includes banks, MFIs, e-money issuers, payments and transfers companies, commercial and consumer credit providers, and agents that provide financial services. The directive uses the following term for agents: *les apporteurs d'affaires aux institutions financières*. Also, professionals such as accountants, auditors, lawyers, and notaries are included for most purposes (art 5). Each WAEMU member state is to maintain a financial intelligence unit (FIU) under Ministry of Finance supervision but with financial and operational autonomy. The FIU (*Cellule Nationale de Traitement des Informations Financières* or CENTIF) is charged with collecting, analyzing, and sharing information on sources of funding flows reported in mandatory filings and related AML/CFT issues (arts. 59–60). Member states are to have supportive legislation (Côte d'Ivoire enacted a law in this field in 2005).

Côte d'Ivoire is making efforts to meet international standards in this area. It is not a member of the Financial Action Task Force (FATF), but it does lead the Inter-Governmental Action Group against Money Laundering in West Africa (GIABA). The latter, a network of FIUs within WAEMU, coordinates institutional reforms to strengthen AML/CFT in the region.

a. *Directive N° 02 /2015/CM/UEMOA du 2 juillet 2015 relative à la lutte contre le blanchiment de capitaux et le financement du terrorisme dans les états membres de l'Union Economique et Monétaire Ouest Africaine (UEMOA).* This is supported by a parallel enactment of the Council of Ministers of UMOA: *Décision N° 26/CM/UMOA du 2 Juillet 2015.*

55 *ARTCI Bulletin de Veille Electronique, 1er trimestre 2016, identifiant unique en Côte d'Ivoire.*

and to compile a database of all mobile services customers.[56] The ID requirement was formalized in a 2011 decree that prohibits the sale of prepaid SIM cards and the activation of any SIM card without prior customer ID.[57] Mobile phone and internet services providers must check a valid form of ID from every individual customer and record her/his full name, place and date of birth, address (postal and physical), phone number, occupation, and details of ID document (this information is not available from a central database).[58] Acceptable forms of ID must have a photo and may include national ID cards, passports, driver's licenses, refugee cards, and professional or student IDs. Copies of records and ID are to be kept for three years.

Côte d'Ivoire's telecoms ordinance affirms these requirements for all operators and providers of telephone and internet services. It requires the same of any third-party agents involved in signing up customers; it places a corresponding duty on subscribers.[59] Services providers/operators are also required to report their numbers of subscribers, monthly, to ARTCI.[60]

Thus, two tendencies are at work here. On the one hand, Côte d'Ivoire is in the process of expanding its ID system to provide something akin to universal coverage. This will relieve a constraint that traditionally excluded large portions of the population from access to financial services. In parallel, ID requirements for access to mobile phones and other digital information channels are becoming stricter and more uniform. Indeed, ARTCI has undertaken a review of these ID requirements, which are expected to be tightened further. The financial sector has its own, mainly regional, standards for customer ID.

5.2 Know Your Customer

This section addresses customer ID requirements relevant to DFS. The adjustment or tiering of these requirements to accommodate financial inclusion is discussed in the next section.

KYC procedures are spelled out in the 2015 WAEMU directive on money laundering.[61] Before any business is transacted, all covered entities must identify their clients—both individuals and organizations. This means obtaining the client's full name, place and date of birth, and primary address, and verifying these by checking a valid "official document" with a photograph (to be copied) and documented proof of address. In addition, merchants must present a copy of their business registration.

Under the AML/CFT directive, ID information is to be collected at various points of the business relationship and retained. This applies to the opening of accounts, fund transfers, and establishment of a business relationship. Full or enhanced KYC is required when there are frequent cash transactions or when there is any suspicion of money laundering, terrorism financing, or use of false documentation. Covered entities must continuously collect and update specified client information for the duration of the business relationship. Additional

56 *La Lettre de l'ARTCI*, July 2010, http://www.artci.ci/.

57 *Décret no. 2011-476 du 21 décembre 2011 portant identification des abonnés des services de télécommunications ouverts au public.* The requirement was carried over into the 2012 telecoms ordinance.

58 A person applying for a subscription on behalf of another person must present the original IDs of both.

59 *Ordonnance no. 2012/293 Relative aux Télécommunications et aux Technologies de l'Information et de la Communication,* arts. 163, 166. Acceptable forms of ID are listed in a separate decree.

60 World Bank, *IOBs* (2016). ARTCI is also reported to be drafting a revised version of the ID decree.

61 Arts. 18–29, 32–33, 40.

AML/CFT precautions are to be taken in the case of most e-transfers. Here, FIs must, in addition to obtaining and verifying the information mentioned, record any FI and account number being used for the transfer and include the client's identifying information in the message accompanying the transfer. Extra precautions are also required for many transactions by occasional clients (i.e., above a threshold of 10 million FCFA [~US$17,000] or where the client is not physically present).[62] Anonymous accounts or those under assumed names are prohibited.

The 2015 BCEAO instructions on e-money and rapid funds transfers stipulate that services providers addressed by those instruments must identify their clients and that these providers are subject to regulations in effect dealing with AML/CFT. The rapid transfer/OTC providers must comply with the KYC ID requirements and the provisions on transactions thresholds (rapid transfer instruction, art. 5).[63] E-money issuers are required to identify new clients by means of an "official document" (art. 27), subject to a limited exception (see Section 5.3). The issuers must supervise their agents and subagents and ensure that there are security and monitoring provisions sufficient to meet standards in the AML/CFT regulations (e-money instruction, arts. 18, 26). The agents have a duty to inform their principal issuers of any e-money dealings that are suspected of having links to money laundering (which the issuers are then to report to CENTIF).

The AML/CFT directive addresses two further issues that are relevant in the DFS context—use of agents and required internal safeguards. On the first point, covered entities are permitted to outsource client ID and oversight while retaining ultimate responsibility for these obligations (arts. 56–58). Agents must be covered entities or relevant professionals (e.g., accountants, lawyers) based in WAEMU, or others approved by BCEAO. The agent must promptly make the client ID information available to the principal FI, which can then share it with partner institutions in WAEMU or elsewhere with equivalent protections for client data.

As for internal corporate safeguards, all covered institutions are required to train their personnel and establish control systems—including centralized information systems and responsibility and procedures for treatment of suspect transactions—to ensure compliance with AML/CFT obligations (arts. 23–25). Additional internal controls are required for FIs, to be further specified by regulation (arts. 35, 90–91). These must include risk classification systems based on factors such as types of services and clients, monitoring and audit procedures to deal with risk, and appropriate standards for personnel recruitment. Risk assessment and management procedures are to be specified and applied within the FI and its branches and affiliates. Client ID documentation must be preserved for 10 years from the end of the relationship or transaction.

In the absence of appropriate tiers or exceptions, the rules just discussed would be disproportionate to the risks involved in small transactions. The rules would also tend to exclude low-income persons who may not be able to meet the ID requirement (although this is becoming less of a problem with improvements to the ID system).

62 Added precautions are required for certain international transactions and where there is an effort to protect anonymity.

63 Transfers are also subject to the banking law, the regulation on international financial relations (09/2010/CM/UEMOA), and the earlier AML/CFT directive (*Directive n°07/2002/CM/UEMOA du 19 septembre 2002 relative à la lutte contre le blanchiment de capitaux et le financement du terrorisme (LBC/FT) dans les Etats membres de l'UEMOA*).

5.3 KYC tiering

Striking the right balance in KYC requirements means taking a risk-based approach in which standards are graduated or tiered to accommodate financial inclusion. The 2015 WAEMU directive on AML/CFT provides some risk-based accommodation in the form of lighter-touch KYC, but does not create KYC tiers.[64] The directive only varies the way in which ID requirements are applied rather than providing exceptions for clients without official ID documents.

Thus, for example, where the risk of money laundering is low (this is to be spelled out in regulations not yet issued), client ID can be carried out during the establishment of the business relationship rather than fully in advance. Also, the continual oversight and updating of client information in the course of the business relationship can be reduced in intensity if AML/CFT risks are low. These oversight and updating procedures can be dropped altogether for certain small transactions by FIs, listed companies, and government agencies.

Covered entities, moreover, can be permitted by regulation (defining the relevant circumstances and categories of institutions) to forego identifying a client and/or beneficiary of online payment services when they determine that risk is absent (arts. 46–48). This applies where the client's funds originate from an account opened under her/his name at an FI based in WAEMU, or another country with equivalent AML/CFT safeguards, and the funds are being sent to an account that meets comparable standards. The transfer may not exceed 150,000 FCFA (US$255), and the client's transaction total for the year may not exceed 1.6 million FCFA (~US$2,700).

Electronic transfers by FIs on behalf of clients are, in principle, subject to less stringent requirements (art. 33).[65] The institution is required to record and verify the client's full name and *either* the client's address, national ID number, or date and place of birth (in addition to the account number, if available). The numbers of any accounts used by the sender or recipient are also to be recorded. These requirements do not apply where an e-funds transfer is made with a credit or debit card or by mobile telephone, provided the transfer is for the purpose of paying for goods or services and the card or phone number is included in all relevant transfer messages.[66] In any case, these provisions deal with transaction-specific checks to be carried out *in addition to* the ID steps required by arts. 27–29 of the AML/CFT directive.

E-money issuers, as mentioned, are required under the 2015 e-money instruction to identify new clients by means of an "official document." The instruction permits the issuer to make an exception for customers engaged in small e-money transactions (up to 200,000 FCFA [US$340] of e-money per month, per customer). However, in the case of mobile money, those customers would already have had to undergo an ID process to obtain SIM cards. Further, the WAEMU directive on AML/CFT, which takes precedence over the BCEAO e-money instruction, does not authorize an ID exception for small transactions (although other limited carve-outs are permitted, as mentioned).

Overall, the KYC provisions that accommodate low-risk clients and transactions are not of the type that advance financial inclusion. In its specific application to e-money issuers, the AML/CFT directive in effect nullifies the exception for small e-money transactions.

64 Arts. 19, 20, 29, 33, 46–48.

65 This refers to a *virement électronique* or transfer between accounts at different FIs (AML/CFT directive art. 1).

66 Also exempt are transfers between FIs for their own account and payments to government.

6. CONSUMER PROTECTION

As with financial services generally and especially in the context of reaching the unbanked, the sound development of DFS hinges, to a large extent, on appropriate protection of consumers. Because consumer risks are heightened in this context well-designed protections are needed. Three critical components of this have already been mentioned: the safeguarding of client funds, the regulation and oversight of agents, and security of e-signatures and e-commerce channels. There remain three further important elements: (*i*) fair and transparent dealing, (*ii*) channels for consumer complaints, and (*iii*) treatment of client data.

In the WAEMU region, consumer protection is treated generally as a matter of national jurisdiction, while financial services and the rules protecting clients in that context are defined at the regional level (WAEMU/BCEAO). Commentators in Côte d'Ivoire have lamented the lack of an effective consumer law framework (Issa-Sayegh 2003). However, this is changing as protections are written into competition and financial regulations, and as Côte d'Ivoire moves toward implementation of new consumer legislation. In January 2017, Côte d'Ivoire adopted a new law on consumer protection (*Loi ivoirienne n° 2016-412 du 15 juin 2016 sur la consommation*) that includes a chapter on financial consumer protection (FCP).[67]

While this is a positive step, best-practice jurisdictions generally place FCP issues under the authority of the banking supervisor or another agency specializing in financial services. Gaps and problems arise in some countries (e.g., Zambia [World Bank 2012]) where the general consumer regulator has authority in this area but does not have the technical expertise (or the interest) to regulate financial services. At least for now, the main protections for DFS clients in Côte d'Ivoire are those contained in the legal-regulatory provisions on financial services (regional) and e-transactions (national). The new consumer legislation in Côte d'Ivoire should offer additional protections and oversight, but it has not been implemented yet. (See Table 3 for an overview of DFS consumer protections.)

6.1 Transparency and conditions of services

Initiating a DFS transaction or relationship raises issues of account opening and transparency of terms. What information must be disclosed to the consumer at the time of opening an account or making a one-off payment or transfer? The 2015 e-money instruction (arts. 29–30) requires a signed contract between the issuer and customer for purposes of opening an e-money account.[68] But there is no requirement to provide a copy of the contract to the consumer, and discussions with customers in the region indicate that this has caused problems. Mandatory provisions include disclosure of the limits, risks, and caution required in using e-money and the procedures in case of fraud, loss, and claims for reimbursement. The issuer is also required to make its fee schedule easily accessible to all customers. In practice, however, the effect of this protection is limited because the customer is not entitled to a copy of the schedule and does not receive a "prompt" with the relevant fee before a transaction is executed. The e-money instruction mandates the issuance of an

67 See the latest draft version available on the Ministry website (http://www.commerce.gouv.ci/commerce/userfiles/file/Loi_relative_a_la_consommation.pdf); BCEAO comments.

68 The instruction appears to accommodate either physical or e-signatures, but in current practice BCEAO requires hard copy.

TABLE 3. DFS consumer protection

Regulatory features	WAEMU and Côte d'Ivoire provisions (WAEMU rules apply unless otherwise stated)
Consumer protection rules for DFS	A patchwork of consumer protection rules applies to DFS. E-money, banking, microfinance, payments, and e-commerce legislation (Côte d'Ivoire) provide some protections for DFS consumers. New consumer legislation (2017) in Côte d'Ivoire may prove helpful.
Information on all costs and fees	*WAEMU:* E-money issuers to make their fee schedules easily accessible to all customers, and e-money agreements to state the conditions for use of the e-money-related services being provided. Rapid funds transfers agents to post their tariffs at teller windows. For payment services, conditions for the use of instruments and accounts to be clearly explained to the customer at the time the account is opened and incorporated in the agreement. MFI law requires transparency in fee arrangements. *Côte d'Ivoire:* E-commerce law provides standards on advertising, offers, contract provisions, transparency of prices (including fees and taxes), and disclosure of identifying information on the seller of goods and services. The new consumer law would strengthen these protections.
Contracts, transparency, provisions	*WAEMU:* Signed contract required between the issuer and customer for opening an e-money account. Application for e-money authorization requires a copy of the draft contract with customers. Agreements must address points such as the respective obligations of the issuer and client, limits and risks of using e-money, procedures in case of fraud or loss. For payment services, conditions for use of instruments and accounts to be clearly explained and incorporated explicitly in a written agreement. *Côte d'Ivoire:* For e-commerce, contractual provisions and procedures for acceptance are to be spelled out clearly. Electronic means of contracting may be used in the case of a consumer, provided the latter accepts this mode of communication.
Complaint handling	E-money issuers are required to set up forums for complaint handling, for both clients and their counterpart e-money acceptors. These systems must be accessible by multiple communication channels at all times, establish deadlines for resolution of claims, and track all complaints received and addressed. But the instruction does not provide for uniform procedures or minimum standards. (Other regulations, including on rapid transfers, are silent on this.) *Observatoire* now being set up in Côte d'Ivoire will provide mediation services and comparative analysis.
Information requirements for agents	E-money issuers to ensure that their agents post visible, legible information that provides information such as name and contacts for the principal issuer. Duty of issuers to make fee schedules easily accessible to all customers applies by implication to agents. Rapid funds transfer agents to include the logo of their principal FIs on their signage and to post tariffs at teller windows.

(Continued)

TABLE 3. DFS consumer protection (Continued)

Regulatory features	WAEMU and Côte d'Ivoire provisions (WAEMU rules apply unless otherwise stated)
Agent fraud	The e-money instruction requires agents to ensure the traceability of transactions and to keep an operational journal that includes any fraud uncovered and any complaints from clients. Issuers are required to have appropriate internal control and risk management procedures—and to ensure that their agents do as well. Banks and MFIs are legally responsible for acts of their rapid transfer agents, although fraud is not explicitly addressed.
Mandate of high-quality performance	E-money and payments rules include standards on prompt crediting of transfers and reimbursement of e-money counterpart funds, irrevocability of electronic orders, and providing account statements to customers. E-money digital platform must be easily available and highly reliable. Payment services customers have the right to a minimum standard of service, including access to secure means of making and receiving payments and transfers.
Data sharing and data authorization procedures	*WAEMU:* The e-money instruction requires issuers to protect clients' personal data in accordance with national and regional legislation. Banking and MFI laws impose a duty of confidentiality on staff, management, and auditors of these institutions. Recent legislation on credit information bureaus contains further provisions on handling of client data in financial transactions. *Côte d'Ivoire:* Personal data protection legislation requires prior consent for collection and handling of personal data. Entities that handle, store, or transmit personal data must be authorized by ARTCI. Telecom legislation requires services providers to protect personal data and confidentiality of communications.

e-receipt for all transactions and specifies the details to be included in it (art. 30).[69]

The 2002 payments regulation sets forth certain additional consumer rights and protections (arts. 8, 10, 14, 15, 142). The conditions for the use of payments instruments and accounts must be clearly explained to the customer at the time the account is opened, and must be incorporated clearly in a written agreement. Customers have the right to a minimum standard of service, including access to secure means of making and receiving payments and transfers, and management of the account, including quarterly statements. The regulation defines the interval between the arrival of a payment order and the crediting of the beneficiary's account.[70] It also stipulates that payments orders are irrevocable, but can be withdrawn in case of fraud (based on the client's appeal, including by telephone). Licensed payments companies and other providers of such services, including the Post, are subject to these rules. [71]

Standardization of these e-money and payments contracts, however, is not practiced or required. This can make

69 The following are to be recorded: reference number and time of the transaction, type of service, issuer name, registration of agent/subagent, identity of recipient, and amount of transaction and fee.

70 A maximum of five days, including preparation, settlement, and float periods.

71 As mentioned, the lack of clear definitions of accounts and services can undercut these FCP protections in practice. Without standard definitions, providers designate services at their discretion, making it difficult for customers to compare terms.

comparison unduly difficult. Nor is there any requirement regarding format (e.g., length or font requirements) or language (e.g., plain language or local language). Results of a customer poll indicate that this is a problem. A concern of special relevance to DFS is the application of consumer protections to agents. Among financial services legislation, only the e-money and rapid transfer instructions have provisions dealing to any extent with this. The e-money instruction (art. 18) requires issuers to ensure that their agents post visible, legible information that includes name and contacts for the principal issuer, for example.

It also holds issuers legally responsible to clients and other third parties for the agent's performance of delegated services (notwithstanding any agreement to the contrary), as well as for the integrity and traceability of transactions conducted by agents. Here again, the Post comes under these rules when acting as an agent for e-money issuers. Similarly, the rapid transfers instruction (arts. 6, 9) requires agents to display information on their principals and to ensure the agents' compliance with the instruction and other regulations. These OTC providers are to include the logo of the FIs they serve on their signage and post their tariffs at the teller windows.

Other basic consumer provisions appear in the banking and microfinance laws.[72] These rules become relevant to DFS when the FIs act as issuers and when customers access their accounts digitally.

Côte d'Ivoire's regulations on e-services offer additional protections. The 2013 e-commerce law provides standards on advertising, offers, contract provisions, transparency of prices (including fees and taxes), and disclosure of identifying information on the seller of the goods and services. The law's provisions on acceptance of electronic offers require that contractual provisions and procedures for acceptance be spelled out clearly. Electronic means of contracting may be used in the case of a consumer, provided the consumer accepts this mode of communication. E-document security, archiving, and other matters are also covered.[73]

As mentioned, a consumer law has been enacted in Côte d'Ivoire. The Commission created by the law is to have units dealing with abusive agreements, consumer protection and security, and over-indebtedness. Specific rules on consumer and housing finance deal with effective interest rates, over-indebtedness, collection, and other issues. The law also sets up a credit registry under BCEAO management to record and share consumer credit data (*incidents de paiement*, i.e., negative information) with credit institutions.

6.2 Complaint channels

Pending implementation of the consumer protection law, and the commission provided therein, FCP complaints are addressed in explicit terms only in the e-money instruction (art. 30). There, issuers are required to set up forums for complaint handling, for both clients and their payees. These systems must be accessible by multiple communication channels at all times, establish deadlines for resolution of claims, and track all complaints received and addressed. The provisions on complaints are not spelled out in detail. Procedures are not standardized, nor are providers

72 Under the banking law (e.g., arts. 15, 56) protection of customer rights is one of the criteria considered by BCEAO in approving licenses. The MFI law (e.g., arts. 60, 81) requires transparency in fee arrangements, and an instruction on internal control requires MFIs to have codes of conduct for dealing fairly with customers (among others), *Instruction n° 017-12-2010 relative à l'organisation du contrôle interne au sein des systèmes financiers décentralisés.* Last, the 2010 IOB instruction makes the principal bank wholly responsible for the actions of its IOB agent, and the principal bank must repair any damage caused. The IOBs are to be provided professional IDs bearing statements to this effect.

73 The 2012 telecoms ordinance is also relevant, as discussed in Section 3.

required to inform consumers about how their complaints are to be handled. Equivalent provisions do not exist under the regulations on payments and transfers.

BCEAO's regional financial inclusion strategy envisions that the Senegal *Observatoire* model will be replicated in other WAEMU countries. Côte d'Ivoire is now setting up its *Observatoire* pursuant to a regulation in January 2017. The Côte d'Ivoire *Observatoire* is to have dispute mediation and comparative analysis functions, and will require focal persons in each regulated entity. Further, this *Observatoire* will allow for functional comparison between institutions that offer transfer services (including between banks, MFIs, and EMEs), and institutions offering transaction accounts (including between banks, MFIs, and EMEs). The World Bank is supporting the Ministry of Finance in establishing this institution.

6.3 Client data protection

Data protection—a major concern for DFS—is covered by general provisions on confidentiality and personal data security in banking, microfinance, and e-money regulations.[74] Regional legislation on credit information bureaus contains further provisions on handling of client data[75]—which will be increasingly relevant to DFS as loans become more widely accessible by digital means.

Côte d'Ivoire has adopted protections for customer data in its 2012 telecoms ordinance, the 2013 law on e-transactions, and the personal data legislation of 2013.[76] These acts are enforced by ARTCI. The laws do not explicitly target financial data or information collected in financial transactions. But they do cover types of sensitive data likely to be handled in DFS operations, such as identity, biometric, household, and legal information. The 2013 data protection legislation requires prior consent by the affected person for the collection and handling of personal data. Entities that handle, store, or transmit personal data must be authorized by ARTCI.

The 2012 telecoms ordinance requires services providers to protect personal data and ensure the integrity and confidentiality of communications (including by their agents). As mentioned, MNOs are providing mobile platforms and the agent networks for mobile money services. Those platforms and associated digital transmissions fall within the authority of ARTCI and the standards on telecoms, data protection, and e-commerce. At the same time, BCEAO regulates e-money issuance using this and other channels. This overlap of authority is still under discussion between the two agencies.

74 The laws on banking (arts. 30, 53–4) and MFIs (arts. 28, 37) impose a duty of confidentiality on the staff, management, and auditors of these institutions. In both cases, an exception is provided for sharing information with the regulator. The e-money instruction simply requires issuers to protect clients' personal data in accordance with national and regional legislation.

75 *Loi uniforme portant règlementation des bureaux d'information sur le crédit dans les états membres de l'Union Monétaire Ouest Africaine (UMOA) 2013; Instruction N° 002-01-2015 relative aux modalités d'obtention du consentement du client par les fournisseurs de données aux bureaux d'information sur le crédit (bic) dans le cadre du système de partage d'information sur le crédit dans les états membres de l'UMOA.*

76 *Loi no. 2013-450 relative à la protection des données à caractère personnelle. Also, Décret no. 2015-79 fixant les modalités de dépôt des déclarations, de présentations des demandes, d'octroi et de retrait des autorisations pour le traitement des données à caractère personnel.*

7. COMPETITION AND COORDINATION

The potential of DFS to increase volume, efficiency, and inclusiveness in the financial system depends on connectivity among relevant communication channels and accounts. Two important constraints in Côte d'Ivoire, as in other settings, are uneven access to mobile communication channels and limited interoperability between competing DFS providers and their networks. These issues are being addressed in part by market players under the guidance of the regulators. More comprehensive solutions will require coordination between financial, telecom, and competition regulators at national and regional levels. This is especially true where, as in Côte d'Ivoire, the DFS market is made up of diverse providers who fit into several regulatory niches with differing requirements—a trend worthy of encouragement but also of coordinated oversight. (An overview of key provisions is given in Table 4.)

7.1 Interoperability

Early rapid growth of one DFS provider tends to defer the advent of interoperability, in turn favoring dominant actors and limiting competitive growth. Thus, an interoperability policy or scheme is often essential for competition in these markets, but in most settings, it is absent or incomplete. It is often difficult to have voluntary agreement on interoperability in the near term, especially where there is a dominant provider. But interoperability can emerge when market players understand the potential shared benefits of network effects. BCEAO has developed a "road map for interoperability," and it benefits from support by the African Development Bank and the Gates Foundation for implementation.

DFS in Côte d'Ivoire and the WAEMU region could be described as comprising closed loops and distinct operating standards, with limited but growing interoperability. A prime example of evolving integration in the region is GIM-UEMOA, a regional switch for ATM and POS payments. This switch is available to EMEs across the region. Several are now GIM-UEMOA members and have access to the switch, including Orange in Côte d'Ivoire. MFIs in the region are slated to get access to this switch, which could also be made available to all e-money

TABLE 4. Interconnection and interoperability

Regulatory features	WAEMU and Côte d'Ivoire provisions
Interconnection (e.g., sharing USSD channel)	*Côte d'Ivoire:* Telecoms legislation states that network access, interconnection, and sharing of essential infrastructure should be provided on an equal, nondiscriminatory basis. Refusal to share essential infrastructure can be deemed anti-competitive, while dominant providers (25% market share) have a duty to offer interconnection. ARTCI is now requiring MNOs to open the USSD channel to external services providers.
Interoperability	*WAEMU:* E-money issuers must ensure that they take the necessary technical and operational steps to facilitate interoperability with other payments systems. Compliance with this requirement is to be verified by external audit every three years, and the audit must cover the issuers' technical partners, who may serve as agents for issuance of e-money.

issuers, but few have shown interest. By contrast, it is reported that ATMs have achieved near total interoperability across Côte d'Ivoire and the region, but not as much progress has been achieved with POS. There are also concerns about interchange fees, irrevocability of transactions, and protection from bankruptcy (World Bank 2014, 39–40, 98–101). Importantly, on the positive side, the 2015 e-money instruction requires issuers to facilitate interoperability.

7.2 Channel access

Another typical constraint to DFS expansion arises from the lack of reliable access to mobile messaging channels. The MNOs control the SIM card with its identity data on each mobile user and the phone's communications channels, including the USSD channel—the one most used by DFS providers. Although mobile money providers depend on USSD, that channel is of minor commercial importance overall for MNOs and telecom regulators. Given its importance to low-cost outreach of DFS, access to this channel is both a competition and financial inclusion issue (Mazer 2015; Hanouch and Chen 2015; Mas 2012; Coye Benson and Loftesness 2012; ITU 2017).

MNOs are not only providers of the channel for mobile money services; they are also competitors (through their EME affiliates) of FI issuers and of EMEs that are not affiliated with MNOs. There is a risk that MNOs will transfer market power from their core market to the emerging mobile money market in such a way as to effectively shut out others. This gives MNOs an opportunity to price-discriminate against financial services providers that are seeking access, or even to deny access, and to favor aggregators that bring them a large volume of business. This is in addition to the more common incentives to squeeze competitors' margins. For their part, MNOs want to protect the privileged access that they gained with their licenses, and to prevent network overload if they share access.

There are reports from Côte d'Ivoire that MNOs have denied USSD access. In other cases, MNOs are reported to have charged heavily for access or limited it in terms of time or connection quality. It is also significant that MNOs are providing channel access to their e-money subsidiaries while restricting access to others.

7.3 Regulatory responses

The frameworks for financial, telecom, and competition regulation—at national and regional levels—provide relevant standards that might be used to address the issues just discussed. BCEAO, of course, has an important role to play here, particularly on *interoperability*. There are sector-specific competition standards embedded in the financial services legislation, and the e-money instruction (art. 7) requires issuers to facilitate interoperability.[77] There has not yet been a strong regulatory push to ensure that different participants in DFS can play together on the same level playing field. Where interoperability does not emerge in the near term from market incentives, the regulator may need to step in. But most observers favor suasion over coercion. Introducing, or mandating, interoperability too early may be counterproductive—it could drive up compliance costs and technical complexity (di Castri 2013; GSMA 2010; Mas 2012). Through its "roadmap for interoperability," BCEAO is showing its commitment to secure full

77 All e-money solutions must ensure platform availability/access (*une haute disponibilité de la plate-forme*), nonrepudiation of transactions, and arrangements (including technical features) that facilitate interoperability with other payments systems. These dispositions are to be checked by way of audits conducted at least once every three years.

interoperability (through GIM-UEMOA) when the market is ready.

ARTCI has authority to approve rates and enforce tariff transparency on behalf of MNO customers. It also regulates value-added services—such as adjuncts to core telephone and data services, and the evaluation of the appropriateness and terms of such services. ARTCI's authority extends to the digital networks used for payments and transfers and the postal service, which provides funds transfer services. Further, ARTCI is responsible for enforcing the laws governing e-commerce and e-signature certification. The agency is tasked with establishing an appropriate mechanism for consumer complaints and follow-up and with ensuring quality of service and effective and fair competition (in cooperation with other relevant authorities).

Clearly, ARTCI's authority over mobile providers and e-commerce overlaps with that of BCEAO. This overlap argues in favor of a framework for coordination. ARTCI is mandated to cooperate with other regulatory bodies in Côte d'Ivoire and the region to regulate competition in the telecoms and data markets, ensure interconnection and quality services, and protect consumers. At the same time, BCEAO is authorized under financial legislation, such as the e-money instruction, to bring in other regulatory authorities to carry out joint inspections. In the DFS context, ARTCI and BCEAO have established a joint working group that is analyzing several areas of concern, including interoperability. ARTCI is also developing a framework for collaboration with the national and regional competition agencies to monitor the development of the telecom sector.

Both Côte d'Ivoire and WAEMU have adopted general regulations on competition and set up regulatory agencies. The WAEMU competition legislation provides standards for identifying and addressing anti-competitive agreements, abuses of dominant position, and other offenses.[78] The regional commission is authorized to make exceptions where such arrangements are found to be (or can be made) efficient and equitable in practice. The Ivoirian legislation[79] contains similar provisions. It also prohibits predatory pricing, and it authorizes price regulation for necessary goods and services. It is not clear how effective these agencies are. In particular, it is reported that the regional-level authority lacks capacity to act swiftly to address anti-competitive practices.

As for access to the USSD channel, the regulatory options in general include the following (Di Castri 2013; ITU 2016):

- The telecom regulator could require open USSD access by MNOs on a nondiscriminatory basis, while perhaps also setting price and quality standards.
- The financial regulator could condition e-money issuance approval on each of the relevant MNOs' giving USSD access to all DFS providers.
- The competition regulator could take jurisdiction if the problem is not solved by market actors or the sector regulators. This will likely depend on showing that a given MNO has abused its dominant market position and that USSD is an essential services infrastructure that must be openly available for there to be a market.

78 The 2002, WAEMU competition law established the regional agency *Département du Marché Régional, du Commerce, de la Concurrence et de la Coopération* (DMRC).

79 *Ordonnance no. 2013/662 Relative à la Concurrence*, establishing *La Commission de la Concurrence et de la Lutte contre la Vie Chère*.

Côte d'Ivoire has chosen the first of these options. ***ARTCI announced in early April 2017 that it is now requiring MNOs to open the USSD channel to external services providers and to make public their respective access offer with a price list. ARTCI was reviewing these prices at the time of this diagnostic. It should continue to monitor MNOs for potential discriminatory pricing and services quality, and scrutinize USSD offers to prevent undue denial of service or prices that are out of line with those of other channels.***

ARTCI has a firm legal basis for its intervention. The telecoms legislation states that network access, interconnection, and sharing of essential infrastructure should be provided on an equal, non-discriminatory basis.[80] Refusal to share essential infrastructure can be deemed anti-competitive, while dominant providers (25 percent or greater share of "pertinent" market) have a duty to offer interconnection. ARTCI is required to monitor conditions of access (which are to be published by the operator) and may enforce access as a last resort. Where there is no effective competition, ARTCI reserves the right to set limits on fees. Denial of sale, price discrimination, and agreements in restraint of trade are prohibited.[81] The competition law provisions mentioned provide additional support for intervention if needed.

80 *Ordonnance no. 2012/293 Relative aux Télécommunications et aux Technologies de l'Information et de la Communication, arts. 16, 18, 35–49*; *Loi no. 95-526 portant Code des télécommunications*, arts. 2.41, 2.42, 2.50, 2.55, 4, 6.

81 *Id.*, arts. 72, 87, 171–74, 180.

8. CONCLUSION

The following is a short distillation of findings and conclusions and recommendations for further policy development. Generally speaking, both WAEMU and the Ivoirian authorities have made impressive strides over the past several years in building an enabling regulatory framework for financial inclusion and DFS, in particular. This effort poses the challenge of ensuring policy consistency and regulatory harmonization—a challenge that is not always met.

Most of the measures suggested are within the responsibility of regional authorities, mainly BCEAO. Recommendations that concern the Ivoirian national authorities (e.g., for some aspects of customer ID and consumer protection) are noted as such.

8.1 E-money and payments

The 2015 e-money instruction has consolidated and clarified the rules in this area. In addition, a sizeable market for payment services has been established under earlier regulations. But questions remain about how supportive of DFS the rules in other, related, areas—such as banking and e-commerce—are. Recommendations are as follows:

- Reconsider the interest rate caps in force across the region. These limits are likely to constrain the offer of innovative digital credit and savings products to the unbanked. At least a partial or phased liberalization is advisable. It would be best to couple this with stricter transparency requirements, including standardized disclosures. This step would support competition, help keep interest rates low, and make it possible to phase out rate caps. As EMEs and OTC providers are not permitted to offer credit under current regulations, the potential sources of digital credit would be licensed credit institutions (e.g., banks) and MFIs.[82]

- Revise the tight limit on MFI activities beyond the traditional ones of savings and credit. BCEAO should grant MFI issuers an automatic exception, or at least a higher limit (i.e., greater than the current ceiling of 5 percent of risk provisions), for earnings from basic DFS activities such as e-money issuance and payments/transfers. A revised regulation should also specify any conditions for such an exception or adjustment (e.g., a defined period of successful operation). Care should be taken to ensure that the rule's prudential objectives continue to be met.[83]

- Clarify protections for e-money float funds. The e-money instruction requires segregation of float funds by the issuer and the depositary institution. However, the treatment of these funds in the case of the issuer's bankruptcy is not clear. It may be advisable to include in the regulations a requirement that funds must be placed in a trust account (as has been done in other countries[84]), to insulate the float from ownership claims

82 An analysis of provider costs and their impact on interest rates could be enlightening in this regard, though it is beyond the scope of this study. According to BCEAO, MFI inspections found that general costs, including salaries, have tended to be out of line with MFI structures and as a result have led to noncompliance with the 24 percent interest rate cap.

83 BCEAO reports that analysis of possible adjustments to this rule is underway. The Bank's chief concern is the protection of MFI depositors.

84 In Kenya and Tanzania, float deposits are required to be placed in a trust account administered by a trustee on behalf of the e-money holder. Trusts are better known in common law than in civil law countries, although the law in this area has been evolving. Thus, Rwanda now requires a trust (*fiducie*) account. A similar arrangement, used in Uganda, is an *escrow* account. This is an account managed by a third party that provides for the isolation of funds until they are released upon the occurrence of conditions stated in the escrow agreement (e.g., authorized payment, settlement).

by the issuer and its creditors. Also, as Côte d'Ivoire's deposit guarantee system goes into operation, it is advisable to clarify its scope of coverage to ensure adequate, equitable protection of e-money float. A uniform system of per-client "pass-through" insurance should be considered (regardless of the type of issuer) to make the guarantee effective for individuals within the coverage limits.[85]

- Harmonize regional and national rules on e-signature acceptance and certification, and ensure coordination and clear jurisdictional lines between BCEAO and ARTCI in this area. It is particularly critical to ensure that certification providers and processes are set up so that fully digital signatures and certifications can be routinely used—without recourse to paper documents, as appears to often have been the case currently. According to BCEAO, work is underway to craft revisions to the regional payments regulation (no.15/2002), including the removal of the requirement to retain physical signatures (art. 19). Region-wide certification is expected to be provided by SOAC, a body established in 2005 by the WAEMU Commission, but which is not yet operational.

8.2 Use of agents

The 2015 instructions on e-money and transfers clarified who can be and who can use an agent, as well as what services agents can provide, while confirming the legal responsibility of the principal. Also important is the recognition of primary agents and subagents; this is a critical step toward the expansion of agent networks within a framework of accountability. On the other hand, the conditions for agent banking appear far too restrictive for the banks and are not clearly articulated for MFIs. In other words, access to agents for distribution of DFS is uneven, creates disparities based on the type of institution (e.g., bank vs. EME), and may act as a drag on financial inclusion and the spread of new DFS products.

Recommendations are as follows:

- Develop uniform, or at least harmonized, agency rules and standards for financial services outreach across the board—including agent banking (for MFIs as well as banks), e-money agents, and rapid transfer agents. A functional, risk-based approach should be adopted, in preference to the current patchwork of mostly institution-based regulation (including IOB rules). The new framework should provide a comprehensive and proportionate set of risk-based rules on due diligence, supervision, internal control, and subagents.

- IOB rules should be revised or replaced to support a more flexible agent banking approach. Further, it would be useful for BCEAO to provide a transition path for e-money agents and rapid transfer agents to enter the market for agent banking services (again, for both banks and MFIs).

8.3 Client identification

The 2015 WAEMU directive on AML/CFT provides a comprehensive set of basic protections in client ID (although the quality of enforcement in practice is less certain). This AML/CFT regime does not sufficiently accommodate financial inclusion and DFS through tiered, risk-based KYC standards. The AML/CFT directive and other regional legislation in such areas as e-money provide

85 An example of this is the system adopted in Nigeria (Izaguirre, Lyman, McGuire, and Grace 2016).

only a patchwork of quite limited (and in some cases conflicting) due diligence exceptions for certain small transactions. Further, mobile money requires a SIM card, which in turn is subject to ID requirements, which appear to be getting more stringent. On the positive side, KYC can be outsourced under appropriate conditions, and Côte d'Ivoire's program of expanding access to official IDs will help ease KYC procedures there and thus enhance financial inclusion.

Recommendations are as follows:

- Replace the patchwork of KYC carve-outs for small transactions (including case-by-case adjustments) with a clear, consistent set of risk-based KYC tiers. The tiers should provide comprehensive coverage of financial services, including DFS, and should provide clearly defined exceptions from requirements more likely to exclude traditionally unbanked groups such as poor and rural populations (e.g., documentation of a permanent address). General FATF principles embodied in the 2015 and 2012 WAEMU legislation also need to be spelled out explicitly in legislation applicable at the national level. The procedure here is to develop a uniform law that incorporates tiered KYC/customer due diligence, and for a WAEMU member country to adopt it into national law—thus leading the way for others.[86]
- Coordinate ID requirements for SIM cards and DFS. The rules should be reviewed so that they can be appropriately graduated to account for the different risks involved in mobile phone subscriptions, payments and transfers, mobile money, and large transactions. This will require cooperation on integrated approaches by the relevant agencies at the national and regional level. One promising approach that could be explored is to carry over the same ID verification procedure used for SIM cards into the KYC process—and perhaps national ID cards and databases as well. (This approach, which is used in Pakistan, depends on having ID data of sufficient quality and using biometrics.) The ongoing improvements in Côte d'Ivoire's ID system should take these needs into account.

8.4 Consumer protection

The consumer protections applicable to DFS are improving, but they are not comprehensive and consistent. Core banking and financial services legislation does little to address consumer protection. But recent enactments on e-money and transfers, e-commerce, and telecoms provide for transparency of fees, complaints handling, required contract provisions, and the like. The new consumer law, with its chapter on financial services, should bring additional, harmonized protections to clients of DFS providers and the financial sector, generally. In addition, data privacy is mandated in the regulations on data protection, credit bureaus, and telecoms. Specific advance consent is required for nearly all potential uses of client data. Importantly, the e-money and rapid transfer regulations apply consumer rules explicitly to agents.

Recommendations are as follows:

- Strengthen and harmonize consumer protections across the full range of DFS—including digital linkage to

86 Jurisdiction over AML/CFT is shared, with WAEMU adopting regional standards and uniform laws and the member countries adopting the latter into national law. Côte d'Ivoire has an AML/CFT law (*Loi no. 2005-554)* that could be replaced, supplemented, or amended in the manner indicated.

savings and credit accounts as this becomes feasible. Protections should include standard disclosure formats and requirements that cover each type of DFS product and delivery channel. Provisions on fraud, security, data protection, and bankruptcy and other contingencies should be similarly expanded. Application of consumer norms to agents should be clearer and more consistent across the board.

- Enhance transparency and comparability by requiring standardized fee information for payments accounts, or at least by introducing standard requirements for format and manner of disclosure.

- A tribunal or ombudsman for retail finance, including DFS, is also important. As mentioned, Côte d'Ivoire is setting up its *Observatoire* pursuant to a regulation of January 2017. Explicit, specific provisions related to DFS will help to strengthen protection in this subsector. Also in January 2017, Côte d'Ivoire adopted a new law on consumer protection. The Commission created by the law is to have units dealing with abusive agreements, consumer protection and security, and over-indebtedness. Here as well, specific provisions on DFS would be useful. Further, the system will be most effective if all financial services providers (not just e-money issuers, as is now the case) are required to have in-house complaint systems, if the latter offer a route of appeal to the Commission and *Observatoire* and if guidelines are provided for appeal to the court system.

- There is a need to make consumer protections effective in practice through systematic supervision. As matters stand, some provisions reportedly are not applied at all by providers. Good practice here involves regulatory oversight of consumer practices as a market conduct and prudential matter.

- Data collection on consumer practices should be strengthened and systematized. BCEAO, along with the consumer commission and *Observatoire,* should require reporting on these matters from FIs, e-money issuers, and agents. Data analysis can reveal patterns of practice as well as risks posed by noncompliance with consumer norms and effectiveness of enforcement.

8.5 Competition and coordination

The inevitable overlaps between markets, services delivery infrastructure, and regulatory regimes create difficulties. The key issues here for Côte d'Ivoire are interoperability and access to the USSD channel. Constraints in these areas tend to work in favor of the dominant provider, and they act as a drag on overall DFS development and financial inclusion. BCEAO and ARTCI have regulatory provisions that they could use to enforce interoperability and USSD access. Importantly, ARTCI announced in early April that it is now requiring MNOs to open the USSD channel to external services providers and to make public their respective access offer with a price list. Also, as mentioned, BCEAO has launched an interoperability "roadmap" with support from external funders.

Recommendations are as follows:

- BCEAO, ARTCI, and perhaps the competition authorities should elaborate on the framework for cooperation that they have discussed, and they should map out a strategy for rationalizing the governance of the DFS market. Recent steps taken by the two regulatory bodies are promising in this regard.

- ARTCI, in cooperation with BCEAO and competition agencies, should monitor MNOs for potential discriminatory pricing and services quality affecting DFS delivery. It should scrutinize USSD offers to prevent undue denial of service or prices that are out of line with those of other channels. Also, BCEAO is responsible for monitoring the price and quality of financial services, including payments services, and has an important role to play here.

RESOURCES

ARTCI Bulletin de Veille Electronique, 1er trimester 2016, Identifiant Unique en Côte d'Ivoire.

Atelier sur les services financiers numériques en Côte d'Ivoire: Compte-rendu, 7 juin 2016.

Bakhshi, Pawan. 2014. "Beware the OTC Trap." Blog post, 9 May.

BFA (Bankable Frontier Associates). n.d. "The Journey toward Cash Lite: Addressing Poverty, Saving Money and Increasing Transparency by Accelerating the Shift to Electronic Payments." Boston: BFA.

BIS (Bank for International Settlements) Basel Committee on Banking Supervision. 2005. *The Joint Forum: Outsourcing in Financial Services*. Geneva: BIS, February.

CGAP. 2016. "Market System Assessment of Digital Financial Services in WAEMU." Working Paper. Washington, D.C.: CGAP.

Coye Benson, Carol, and Scott Loftesness. 2012. "Interoperability in Electronic Payments: Lessons and Opportunities." Washington, D.C.: CGAP.

di Castri, Simone. 2013. "Mobile Money: Enabling Regulatory Solutions." London: GSMA, February.

Gage, Justin, Steve Pannifer, and Paul Makin. 2016. "Country Note: Pakistan." Washington, D.C.: World Bank.

GPFI (Global Partnership for Financial Inclusion). 2016. "Global Standard-Setting Bodies and Financial Inclusion: The Evolving Landscape." Geneva: GPFI. http://www.gpfi.org/sites/default/files/documents/GPFI_WhitePaper_Mar2016.pdf

GSMA. 2010. "Mobile Money Definitions." London: GSMA, July.

Hanouch, Michel, and Gregory Chen. 2015. "Promoting Competition in Mobile Payments: The Role of USSD." Brief. Washington, D.C.: CGAP, February.

Issa-Sayegh, Joseph. 2003. *Le droit ivoirien de la concurrence*, Ohadata D-06-04. Symposium, Ouagadougou, February.

ITU. 2016. "Digital Financial Services: Regulating for Financial Inclusion—An ICT Perspective, GDDFI Discussion paper.

Izaguirre, Juan Carlos, Timothy Lyman, Claire McGuire, and David Grace. 2016. "Deposit Insurance in the Digital Financial Inclusion Context." Brief. Washington, D.C.: CGAP.

Koné, Tiémoko Meyliet. 2016. "Mobile Financial Services Are Making Headway in WAEMU." BCEAO blog post, 14 June.

Lauer, Kate, and Timothy Lyman. 2015. "Digital Financial Inclusion: Implications for Customers, Regulators, Supervisors, and Standard-Setting Bodies" Brief. Washington, D.C.: CGAP.

Lhériau, Laurent. 2010. Le droit et la technologie au service de la bancarisation : focus sur la banque à distance. Techniques Financières & Développement, N°100. Paris: Epargne Sans Frontière, Septembre.

LIRNEasia and UP-NCPAG.2008. "Mobile Banking, Mobile Money and Telecommunication Regulations." http://lirneasia.net/wp-content/uploads/2008/05/Mobile-2.0_Final_Hor_EA.pdf

Mas, Ignacio. 2012. "What Is the Telecom Regulator's Role in Fostering Mobile Money?" Blog post, 8 May.

Mazer, Rafe. 2015. "USSD Access: A Gateway and Barrier to Effective Competition." Blog post, 18 February. http://www.cgap.org/blog/ussdaccessgatewayandbarriereffectivecompetition

McCaffrey, Mike, Graham A. N. Wright, and Anup Singh. n.d. "OTC: A Digital Stepping Stone, or a Dead End Path?" Microsave. http://www.microsave.net/files/pdf/1467712097_OTC_Digital_Stepping_Stone_or_Dead_End_Path.pdf

Radcliffe, Dan, and Rodger Voorhies. 2012. "A Digital Pathway to Financial Inclusion." Seattle: Bill & Melinda Gates Foundation, December.

Rashid, Naeha, and Stefan Staschen. 2016. "Unlocking Financial Inclusion Using Biometrically Verified SIMs." Blog post, 26 July. http://www.cgap.org/blog/unlocking-financial-inclusion-using-biometrically-verified-sims

Staschen, Stefan. 2016. "DFS Regulation and Supervision—What's Going on? What Is Coming up?" Slide deck. Washington, D.C.: CGAP, February.

World Bank. 2012. "Republic of Zambia: Diagnostic Review of Consumer Protection and Financial Literacy." Washington, D.C.: World Bank. https://openknowledge.worldbank.org/handle/10986/25890

———. 2014. "Diagnostic des paiements de détail et stratégie pour développer leur utilisation dans l'UEMOA." Washington, D.C. : World Bank.

———. 2016. *Intermédiaires en opérations de banque et banque à distance: Réflexions sur le cas de l'UMOA*. Washington, D.C. : World Bank, May.

Wright, Graham. 2014. "Over the Counter Transactions—Liberation or a Trap? Part I." Blog post, December. http://blog.microsave.net/over-the-counter-transactions-liberation-or-a-trap-part-i/

ANNEX 1. LEGISLATION CONCERNING DFS IN WAEMU AND CÔTE D'IVOIRE

WAEMU

Avis n° 003-08-2013 aux établissements de crédit et aux systèmes financiers décentralisés, relatif à la fixation du taux de l'usure dans les Etats membres de l'UEMOA, BCEAO.

Décision n° 26/CM/UMOA du 2 juillet 2015 portant adoption du projet de loi uniforme relative à la lutte contre le blanchiment de capitaux et le financement du terrorisme dans les Etats membres de l'Union Monétaire Ouest Africaine (UMOA) Décret d'application de la loi portant réglementation des systèmes financiers décentralisés.

Directive n° 02/CM/UEMOA du 2 juillet 2015 relative à la lutte contre le blanchiment de capitaux et le financement du terrorisme.

Directive n° 07/2002/CM/UEMOA du 19 septembre 2002 relative à la lutte contre le blanchiment de capitaux et le financement du terrorisme (LBC/FT) dans les Etats membres de l'UEMOA.

Directive n° 08/2002/CM/UEMOA portant sur les mesures de promotion de la bancarisation et de l'utilisation des moyens de paiement scripturaux.

Instruction n° 01/2006/SP du 31 juillet 2006 relative à l'émission de monnaie électronique et aux établissements de monnaie électronique (replaced by 2015 instruction).

Instruction n° 127-07-08 fixant les modalités de mise en œuvre de la surveillance par la BCEAO des systèmes de paiement dans les Etats membres de l'UEMOA.

Instruction n° 010-08-2010 relative aux règles prudentielles applicables aux systèmes financiers décentralisés des Etats membres de l'Union Monétaire Ouest Africaine (UMOA).

Instruction n° 011-12/2010/RB relative au classement, aux opérations et à la forme juridique des établissements financiers à caractère bancaire.

Instruction N° 013-11-2015 relative. . . transfert rapide d'argent en qualité de sous-agent au sein de l'UEMOA, BCEAO.

Instruction n° 015-12/2010/RB fixant les conditions d'exercice des activités d'intermédiaires en opérations de banque.

Instruction n° 017-12-2010 relative à l'organisation du contrôle interne au sein des systèmes financiers décentralisés.

Instruction N°008-05-2015 régissant . . . activités des émetteurs de monnaie électronique, BCEAO.

Loi portant réglementation des systèmes financiers décentralisés.

Loi uniforme relative à la lutte contre le blanchiment de capitaux dans les Etats membres de l'UEMOA.

Loi uniforme relative à la lutte contre le financement du terrorisme dans les Etats membres de l'UEMOA.

Loi uniforme relative à la répression des infractions en matière de chèque, de carte bancaire et d'autres instruments et procédures électroniques de paiement (UEMOA).

Loi-cadre portant sur la réglementation bancaire (BCEAO).

Recueil des textes légaux et règlementaires régissant les systèmes financiers décentralisés de l'UMOA.

Règlement n° 09/2010/CM/UEMOA/ relatif aux relations financières extérieures des Etats Membres de l'UEMOA.

Règlement n° 15/2002/CM/UEMOA relatif aux systèmes de paiement dans les Etats membres de l'UEMOA.

Statuts de la Banque Centrale des Etats de l'Afrique de l'Ouest 2010.

Statuts du fonds de garantie des dépôts dans l'Union Monétaire Ouest Africaine (UMOA) 2014.

Textes d'application de la loi portant réglementation bancaire.

Traité modifié de l'Union Economique et Monétaire Ouest Africaine.

Côte d'Ivoire

Décret no. 2014-106 du 12 mars 2014 . . . conservation de l'écrit et de la signature sous forme électronique, J.O. Côte d'Ivoire.

Décret no. 2015-79 du 04 février 2015 fixant les modalités . . . des autorisations pour le traitement des données à caractère personnel, J.O. Côte d'Ivoire.

Loi no. 2005-554 du 2 décembre 2005 relative à la lutte contre le blanchiment de capitaux.

Loi no. 2013-450 du19 juin 2013 relative à la protection des données à caractère personnel, Journal Officiel de la République de Côte d'Ivoire.

Loi no. 2013-451 du 19 juin 2013 relative à la lutte contre la cybercriminalité, J.O. Côte d'Ivoire.

Loi no. 2013-546 du 30 juillet 2013 relative aux transactions électroniques, J.O. Côte d'Ivoire.

Loi no. 2013-702 du 10 octobre 2013 portant Code des Postes, J.O. Côte d'Ivoire.

Loi ivoirienne n°2016-412 du 15 juin 2016 sur la consommation.

Ordonnance no. 2012-293 du 21 mars 2012 relative aux Télécommunications et aux TIC, J.O. Côte d'Ivoire.