GROUPE D'ACTION CONTRE LE BLANCHIMENT D'ARGENT EN AFRIQUE CENTRALE (GABAC)

NEW METHODS OF PAYMENT

FACING THE CHALLENGES OF THE FIGHT AGAINST MONEY LAUNDERING AND TERRORISM FINANCING IN THE CEMAC AREA

AUGUST 2017

Immeuble de la BVM AC - place de l'Indépendance
P.O. Box: 764 Libreville - Gabon - Tel.: +241 01 76 39 54
E-mail: secretariat@spgabac.org - www.spgabac.org

GROUPE D'ACTION CONTRE LE BLANCHIMENT D'ARGENT EN AFRIQUE CENTRALE

The Groupe d'Action contre le Blanchiment d'Argent en Afrique Centrale (GABAC—the Task Force on Money Laundering in Central Africa) is a specialised body of the Central African Economic and Monetary Community (CEMAC) whose missions include:

- Combating money laundering and the proceeds of crime;
- Implementing appropriate measures in a smooth and concerted fashion to support these efforts within the CEMAC;
- Assessing the impact and effectiveness of the measures adopted;
- Assisting member states with their anti-money laundering policy;
- Working with existing African and international organisations.

GABAC has been an associate member of the Financial Action Task Force (FATF) since October 2015.

© 2017 GABAC. All rights reserved
This document may not be reproduced or translated without express permission from GABAC.

OVERVIEW

Within the CEMAC (Central African Economic and Monetary Community), banks, microfinance institutions (MFIs) and mobile telephone operators have, over the last decade, introduced technological and organisational innovations to increase financial inclusion among people who do not have access to financial products in the sub-region. One major advance in this area was the arrival of e-money, which has been made a reality with the use of new payment methods (NPMs) as payment instruments.

However, if the financial transactions they enable are not properly traced, the wide distribution of NPMs can facilitate transactions used in money laundering and terrorism financing.

This typologies exercise, which covers prepaid cards, payments made via mobile telephones (mobile money) and those made via websites, demonstrates that the volume of NPM transactions is undergoing sharp growth in the CEMAC. This growth is more marked in certain member states than in others. In addition, the lack of traceability of payments made via NPMs, inappropriate regulatory and monitoring provisions, and the anonymous nature of the parties behind certain transactions are the main risk factors for money laundering and terrorism financing.

Two known cases of money laundering linked to the use of NPMs in the CEMAC have been identified: one involved money laundering through pre-paid cards, and the other involved the use of mobile money.

As the Bank of Central African States does not have a system for monitoring transactions made via NPMs, the working group in charge of carrying out this study encountered significant difficulties in accessing the data it required, including information held by banks, mobile telephone operators, supervisory bodies and the authorities responsible for monitoring and combating money laundering and terrorism funding ■

CONTENTS

INTRODUCTION

Although a considerable number of financial transactions are made via informal financial systems, the rate of use of the banking system in the CEMAC area—an average of 11%—is an obstacle to the development of commercial transactions (Mayoukou, 2000, Lelart, 2002). The low proportion of the active population with access to banking services does not promote high levels of financial inclusion, a socially and politically sustainable economic growth factor in the long term (Levine, 2003, Adrianaivo and Kpodar, 2012, Babajide, 2015).

In other terms, in CEMAC countries, a significant proportion of the population—excluded from the financial system but economically active—lives outside the formal economy, particularly in suburban and rural areas, where there is a low density of bank branches. In addition, those citizens who do have access to the financial system do not always use the financial services that are available to them.

It is in this environment that banks, microfinance institutions (MFIs) and mobile telephone operators within the CEMAC have, over the last decade, introduced technological and organisational innovations to increase financial inclusion among people living in the sub-region. One major initiative in this area was the arrival of e-money, which has been made a reality with the use of new payment methods as payment instruments.

Regulation 01/11/CEMAC/UMAC/CM defines e-money as "monetary value stored in electronic form and purchased with funds of equal value; e-money may be used to make payments to people other than the issuer without involving bank accounts in the transaction". The e-money instruments covered in this study include pre-paid cards, internet payments, and payments made via a mobile telephone, known as 'mobile money'. These are generally grouped together under the name 'new payment methods' (NPMs).

Despite being relatively late to be adopted in the CEMAC in comparison to other African sub-regions[1], these methods have experienced significant growth since their introduction, both in terms of the number of instruments issued as well as in terms of the volume of transactions carried out.

The adoption of national financial inclusion strategies, drafted by several

1 Kenya is often given as an example. This East African country has experienced some of the most significant development in mobile money in Africa.

CEMAC member states, as well as the adoption and implementation of regulatory texts promoting the development of the supply of and demand for NPMs are encouraging the spread of these financial instruments within the CEMAC. However, it has become clear that inadequate regulatory controls on financial transactions made via NPMs may facilitate money laundering and terrorism financing. These two phenomena are a threat to national financial stability and economic prosperity (Lawack, 2013), in that they can compromise the integrity of the financial system and distort the allocation of financial resources, including by misdirecting investments in the economy thereby creating insecurity, for which some countries in the sub-region pay a heavy price. It therefore seems essential to provide a better framework for NPMs and monitor their use to reduce the risks of money laundering and terrorism financing in a context of worrying levels of instability.

Money laundering is defined in article 1 of Regulation 01/CEMAC/UMAC/CM on the prevention and suppression of money laundering and of the financing of terrorism in Central Africa as follows: *"a) converting or transferring property originating from criminal activity in the sense of the relevant legal texts of the member state or in the sense of this Regulation, with the aim of concealing or disguising the illegal origin of said property or of helping any person involved in this activity to escape the legal consequences of these acts;…[2] "*. Open to a wide customer base, new payment methods could be used as a financial instrument to assist criminals and those guilty of money laundering and terrorism financing.

As with money laundering, terrorism financing is defined in the same Regulation as *"the act by any person, by any means whatsoever, directly or indirectly, illegally or deliberately, of providing or collecting funds with the intention of having them used, or knowing they will be used, in whole or in part: a) with a view to commissioning a terrorist act as defined by any relevant international treaty duly ratified by the member state;"*. In light of this clarification, NPMs could constitute a means of storing, transporting, transferring or making payments using funds intended for terrorist activities. The context in CEMAC member states, in particular Cameroon, the CAR and Chad, in which insurrectionist and terrorist movements such as Boko Haram, Seleka and Anti Balaka operate, certainly requires effective monitoring of the use of NPMs.

OBJECTIVES

Among other aims, and in accordance with its terms of reference, the objective of this typologies exercise is to report on developments in NPMs

2 Regulation 01/CEMAC/UMAC/CM on the prevention and suppression of money laundering and of the financing of terrorism and proliferation in Central Africa of 16 April 2016, article 8a)

in the sub-region and to produce a comparative analysis of a range of regulatory approaches that could be used to regulate and monitor the phenomenon of NPMs that maintain a balance between the need to promote financial inclusion, on the one hand and, fight against money laundering and terrorism financing. It also aims to identify the specific risks and vulnerabilities inherent to the following NPMs: pre-paid debit cards, online payment systems (including virtual money) and mobile telephone payment services. Finally, based on case studies located where possible in the sub-region, this report aims to draw up procedures and to identify trends in the misuse of NPMs for money laundering and terrorism financing purposes in Central Africa.

METHODOLOGY

In light of previous developments, following a workshop seminar on the theme, the Groupe d'Action contre le Blanchiment d'Argent en Afrique Centrale (GABAC) formed a working group which was tasked with carrying out a typologies exercise covering five of the six CEMAC member states[3], which was designed to detect and contain the inherent vulnerabilities to money laundering and terrorism financing that arise from the use of NPMs.

This group was formed of 40 members from national authorities responsible for regulating and monitoring the financial sector, those responsible for criminal proceedings and criminal police investigations (Finance, Justice and Security), credit institutions, mobile telephone companies offering NPMs in countries in the sub-region, financial intelligence units, and regional authorities responsible for monitoring and regulating the financial system in Central Africa (the Bank of Central African States [BEAC] and the Central African Banking Commission [COBAC]).

Information was collected from sub-regional regulation and monitoring bodies, financial intelligence units, national financial sector monitoring and regulatory bodies, prosecution authorities, credit institutions and mobile telephone operators.

The working group produced questionnaires, which were then sent to the administrative bodies and entities mentioned above. Information from the surveys revealed that three (3) questionnaires were filled in respectively by officials of authorities responsible for monitoring and combating money laundering and by regulatory and monitoring authorities. In addition, ten (10) questionnaires were filled out by banking and mobile telephone company employees. The questionnaire data was supplemented by semi-directive interviews with financial system stakeholders. Thirteen (13) interviews with

3 Equatorial Guinea did not contribute to the work

regulation and monitoring agencies were carried out, along with eleven (11) others with banking and mobile telephone company employees. After this information was processed, the proposals of this report were formulated.

This report comprises five chapters: the first is a brief literature review regarding NPMs; the second reports on the current status of NPMs in the CEMAC; the third maps the risks linked to NPMs; the fourth features case studies of typologies; and the fifth and final chapter sets out recommendations.

CHAPTER I

Financial inclusion literature review

Over a billion people live on less than 500 CFA[4] francs per day, and over three billion live on less than 1000 CFA francs. A total of 825 million people around the world, 200 million of whom are children, suffer from hunger, mainly in countries of the global south (Attali, 2006). Most of these people live outside traditional financial systems. However, financial inclusion can be a solution to these individuals' financial problems, and a way to improve their living conditions (Mosley and Hulme, 1996, Helms, 2006).

Microfinance has long been presented as the main way of combating poverty and of ensuring the financial inclusion of excluded people in under-developed countries. By accessing microfinance services, particularly microcredit, the beneficiaries—the vast majority of whom are poor—can carry out income-generating activities (Armandariz de Aghion and Morduch, 2005, Lelart, 2005). With the resulting income, they can meet their basic requirements, such as clothing, food, healthcare, children's education fees, and more.

However, access barriers to microfinance for poor people, which stem from some MFIs' quest for a profit, calls into question the way these institutions target poor people (CGAP, 2001). These barriers also limit the ways in which microfinance can help the world's poorest people and bring about financial inclusion for those who are poverty-stricken (Helms, 2006). As it is primarily commercial, microfinance in Central Africa presents a number of limitations in its contribution to financial inclusion for all citizens (Servet and Fall, 2010).

According to a study by the GSMA[5], the organisation believes that "in many developing countries, mobile operators have been more successful reaching unbanked consumers than banks. Mobile money services are a unique opportunity to move customers who have a mobile telephone but not a bank account from a cash payment system to a formal financial system, which then gives them access to a range of financial services.

"Studies undertaken in several countries, including Brazil, South Africa, Kenya, Malaysia and the Philippines, indicate that their lower cost is one of the most significant factors driving the adoption of new mobile money services. Speed of delivery and convenience are also important, as are the

4 One euro = 655.96 CFA francs
5 Mobile Money for the Unbanked (Maria Solin, Andrew Zerzan, 2009)

perceived safety of the money from loss and the security of the transactions. "Research shows that mobile money brings unbanked customers operating in a cash economy into the formal sector. Once they have developed trust in mobile money services, they start demanding traditional financial services, such as savings accounts (i.e. customers who are previously unbanked start to ask for savings after they have become sophisticated users of mobile money and can be handed over to banks and traditional banking services). Mobile money therefore has the important function of bringing unbanked customers into the formal financial system. On a mass scale, this will result in formalising the financial system and lowering overall ML/TF risk."

Since becoming available, mobile money and other NPMs have facilitated access to financial services for people who are located on the margins of traditional financial systems (Klein and Mayer, 2011, Donovan, 2012, Lal and Sachdev, 2015). Using these new instruments, billions of people worldwide carry out financial transactions (Chatain et al, 2008). Due in part to the dynamic nature of microfinance, the bank account ownership rate is around 20% (higher than the CEMAC average) in Cameroon. Regarding mobile phone use, also in Cameroon, the penetration rate increased from 9.8% in 2004 to 71% in 2014, with 18.6 million people holding subscriptions in total and a potential market of almost 15 million for mobile money[6]. In Gabon, the number of subscribers had risen to almost three million in 2014[7], while the figure in the Republic of the Congo stood at 4.59 million in 2015[8]. In Chad, the mobile telephone penetration rate grew from 0.07% in 2000 to 39.75% in 2014. In these countries, NPMs, and in particular mobile money, promote easy access to financial services for a wide segment of the population who do not have a bank account.

However, it should be recognised that the use of NPMs exposes the financial system to significant risks of money laundering and terrorism financing. These risks are heavily dependent on several factors that determine the nature of their occurrence (Di Castri, 2013). One of the major factors behind these risks is technological failures, leading organisations to implement automated processes. As a result, these processes are not effective at containing the risks mentioned above, as the phenomena being studied are very complex and extremely changeable. The use of these means of mobilising e-money, which is not always linked to a financial institution and which can quickly be moved from one party to another makes it difficult to know the identities of the range of people involved (Demetis, 2010, p. 9). False user identities and the fragmented nature and speed of the transactions, which can be made anywhere

6 These statistics are taken from Investir au Cameroun no. 38, published in June 2015. Several articles in this issue cover the use of mobile money in the country.

7 http://www.lenouveaugabon.com/telecom/1006-9149-gabon-1-million-d-internautes-3-millions-d-abonnes-au-mobile

8 http://www.afrique-it.com/web-tech/analyse-comparative-de-la-telephonie-mobile-au-congo-brazzaville-arpce/

at any time, are also factors that give rise to these risks (Chatain et al, 2008).

The combination of these risk factors in a range of contexts has resulted in a number of typologies of money laundering and terrorism financing. A study of the French context[9] highlighted several cases of money laundering using NPMs. These cases involved (1) the illegal conduct of banking business via a virtual currency that is not legal tender (bitcoin), (2) the complexity of detecting the origin of funds and the distribution of pre-paid cards by a non-transparent actor, and (3) the use of pre-paid cards in a fraud scheme.

In addition, a study of the Korean context focusing exclusively on mobile money led to the identification of money laundering case studies. One such case involved cyber-gambling. A person used a false identity to participate in illegal gambling online. This person used foreign employees and accomplices to deposit profits from gambling in Korean banks. Another case was linked to cross-border money transfers, in which another person, who also used false identities, opened several bank accounts. These accounts were then used to receive significant amounts of money over a short period of time. Funds were sent by several people with false identities, and were then used to make transactions in the form of mobile money. A final case involved fraud via an investment fund, which was created for fraudulent purposes. Investors were attracted by the promise of a high return on investment, and sent considerable amounts of money to the investment fund via mobile money (Chatain et al, 2008, p. 15).

Studies carried out in Europe and Asia demonstrate that the types of money laundering and terrorism financing depend on the area where transactions are carried out. This potential approach to the phenomenon therefore requires special analysis of the situation in the CEMAC to better determine the form that money laundering and terrorism via NPMs may take in the area.

9 TRACFIN, Monnaies électronique, monnaies virtuelles et nouveaux risques [Electronic currencies, virtual currencies and new risks]

CHAPTER II

The current status of new payment methods in the CEMAC

Before considering the phenomena of money laundering and terrorism financing linked to NPMs in the CEMAC, it appears necessary to conduct a review of the way they are issued and distributed in the sub-region in order to be aware of the parties involved, the people who make use of NPMs, the type of financial transactions they enable and the regulatory system and monitoring system that applies to these payment methods.

2.1 Regulations regarding new payment methods

The regulatory system governing NPMs in the CEMAC is part of the process to modernise the payment systems and methods put in place by the Bank of Central African States (BEAC) in 1999 with the aim of modernising these systems and limiting the use of cash in the sub-region. As part of this project, a regulatory framework was created in the form of the following regulations and instructions:

- Regulation N°01/CEMAC/UMAC/UM of 11 april 2016 on the prevantion and the suppression of money laundering and terrorism financing and proliferation in Central Africa,
- Regulation 02/03/CEMAC/UMAC/CM of 04 April 2003 on payment methods and systems;
- COBAC regulation R-2005/01 on diligence by establishments liable on matters of combating money laundering and the financing of terrorism in Central Africa;
- COBAC regulation R-2005/02 on e-money institutions;
- Regulation 01/11/CEMAC/UMAC/CM of 18 September 2011 setting out the conditions for practising the issuance of e-money as well as the roles of the regulating authorities;
- Instruction 01-GR of 31 October 2011 from the Governor of the BEAC on the monitoring of e-money payment systems, with an appendix including a reference framework featuring aspects to allow the BEAC to continue its work of monitoring activity;
- Instruction 02/GR/UMAC of 07 May 2014 from the Governor of the BEAC on the implementation of multibanking as part of the issuance of e-money.

2.2 Changing regulations on new payment methods

The gradual modernisation of payment methods and systems in the sub-region of Central Africa has led to the adoption of e-money. The various forms this takes are called NPMs, and, as previously indicated, include pre-paid cards, mobile telephony (mobile money), and internet payments.

The regulations governing e-money are primarily based on community texts on payment methods. They are supplemented by Regulation 01/11/CEMAC/UMAC/CM, Instruction 01/GR from the Governor of the BEAC, and by Instruction 02/GR/UMAC of 07 May 2014. These texts cover:

- the relevant definitions;
- the purpose and scope of application;
- the conditions for carrying out the practice of issuing e-money;
- the rules for the issuing of e-money and its conversion into cash or scriptural money;
- regulation, supervision and monitoring of the practice of issuing e-money;
- cessation of the practice of issuing e-money;
- transitional and final arrangements.

They define e-money as monetary value stored in electronic form and purchased with funds of equal value; e-money may be used to make payments to people other than the issuer without involving bank accounts in the transaction. E-money is thus mainly characterised as being:

- a claim held by the holder against the issuer, for which the holder can request reimbursement of the remainder or of the value of the unused part;
- an electronic instrument, as electronic systems (pre-paid cards, mobile money, computer servers) facilitate its storage and remote management, as well as its use in financial and commercial transactions;
- a method of exchange that can be used to pay third parties other than the issuer of the e-money or to transfer funds between individuals, or to withdraw cash from an automated teller machine.

They grant the ability to issue e-money to credit institutions exclusively. In addition, they determine the contents of contracts drawn up between the issuing institutions and holders and acceptors, and assign regulation and supervision of this practice to the COBAC and the BEAC. They thus introduce a requirement for these credit institutions to provide information and in-

telligence and extend monitoring of this activity to technical and commercial partners (Ndjimba[10], 2016).

This regulatory framework describes the role to be played by e-money stakeholders and the conditions under which their activity is to be carried out. It is supplemented by multibanking provisions, which permits and regulate e-money transactions involving more than one financial institution issuing electronic money on a Telco e-money platform.. The CEMAC legal framework regarding NPMs is, to give a general overview, similar to that of the ECOWAS, particularly in terms of the conditions for obtaining permission to carry out this practice and the conditions for the practice itself (Ndjimba, 2016). However, the use of NPMs involves risks of various kinds, including money laundering and terrorism financing. Current regulations, supported by regulations adopted by the COBAC, attempt to limit these risks.

2.3 Regulatory provisions regarding the combating of money laundering and terrorism financing linked to new payment methods

Regulatory provisions require anti-money laundering and counter-terrorism financing provisions to be put in place to alleviate the vulnerabilities linked to the use of NPMs. As such, Regulation 01/CEMAC/UMAC/CM of 16 April 2016 on the prevention and suppression of money laundering and of the financing of terrorism in Central Africa and COBAC regulations provide for the adoption of arrangements such as:

- Know Your Customer or KYC: as such, all institutions subject to these requirements take due diligence measures regarding new customers before establishing a business relationship. These involve verification of the customer's identity by requiring a valid original official document, as well as diligence regarding the origin of the funds, the identity of the beneficiaries and those who control the funds;
- knowledge of the customer's business relations: this is intended to estimate the number of commercial relations in which the customer is involved. These procedures must be carried out every time major changes to the customer's business occur. In carrying out these procedures, the institution may assess the legitimacy of the transactions being carried out and, where applicable, detect suspicious transactions;
- monitoring transactions: relevant institutions must constantly monitor their business relations and ensure that their transactions are carefully examined throughout the duration of the relationship. This ensures that the transactions carried out by the customer are consistent with the latest information concer-

10 This document was written by Dr Ndjimba as part of his work with the GABAC. It is included as an appendix to this report.

ning the customer in question, which institutions subject to these requirements must hold. These arrangements are simplified thanks to computerised systems that detect unusual transactions based on the customer's profile;

- declaration of suspicion: institutions are required to appoint at least one NAFI (National Agency for Financial Investigations) and COBAC officer, whose identity is passed on to these bodies; they must declare in writing or orally, if required, any suspicious transaction before or after it has occurred. Within an institution, a manager or agent who is not officially designated is still permitted to declare suspected money laundering or terrorism financing in an emergency;
- centralisation of information regarding the identity of customers, originators and beneficiaries, and regarding transactions. Through these arrangements, each CEMAC member state will create national records including records of incidents linked to payments by cheque and by payment cards, as well as illegal cheques and cards. The information contained in these records is reserved for relevant institutions to be used to profile their customer base, for the criminal police, for magistrates as part of criminal proceedings, for financial intelligence units and for sub-regional and national supervisory and monitoring authorities;
- communication of information: the BEAC and other institutions covered by these requirements must pass on all information that may be useful in suppressing financial crime to financial intelligence units, to the competent criminal prosecution authorities, and to public prosecutors.

A more detailed comparative analysis of the legal frameworks of the CEMAC and the ECOWAS highlights the former's many weaknesses. These are linked to the legal framework surrounding the issuance of e-money and to measures concerned with combating money laundering carried out via NPMs (Ndjimba, 2016).

Regarding the legal framework surrounding NPM offerings, most of the provisions within the CEMAC tend to set out general principles without truly creating actual binding obligations. There is also a lack of provisions regarding the relationships between credit institutions and their partners, a lack of obligations to carry out internal monitoring, and a failure to specify the responsibility of issuing institutions regarding their partners' activities. In addition, the limited nature of the traceability obligation, set at just three (03) years in the CEMAC, whereas in the ECOWAS, this figure stands at ten (10) years, is inadequate.

The CEMAC legal framework is characterised by a void of sorts when it comes to the fight against money laundering and terrorism financing via

NPMs. Unlike that of the ECOWAS, the CEMAC framework does not clearly indicate which of the various parties are subject to the community rules on these phenomena.

It is clear from the above that although the CEMAC's legal framework is designed to give structure to the use of e-money in the sub-region, it does not adequately take into account the aims of combating money laundering and terrorism financing as foreseen in Regulation 01/CEMAC/UMAC/CM of 16 April 2016 on the prevention and suppression of money laundering and of the financing of terrorism and proliferation in Central Africa.

However, alongside an adequate regulatory framework, management of the risks of money laundering and terrorism financing inherent to the use of NPMs also requires in-depth knowledge of the supply of and demand for these instruments in the CEMAC sub-region.

2.4 The new payment method market in the CEMAC

For the last several years, the use of NPMs has been growing in the CEMAC. Although it involves a number of stakeholders, this market is nonetheless in its infancy, just like the traditional bank card market, which is still in the early stages of development.

2.4.1 Pre-paid cards

In the sub-region's banking system, two types of bank cards are in circulation: debit cards, which are linked to a bank account, and pre-paid cards. This study will consider pre-paid cards only.

Debit cards are coupled to a bank account. They allow their holders to withdraw cash from automated teller machines (ATMs) and to make payments, whether to retailers equipped with electronic payment terminals (EPTs), or online to suppliers and banks that offer this type of payment. These cards, which are made of plastic and fitted with a chip, are for the use of the named cardholder, and generally work by entering a confidential personal identification number (PIN). The use of some bank cards may be restricted to a single country or a single banking network. However, cards linked to international payment circuits such as VISA or MASTERCARD may be used anywhere in the world from the time that this feature is activated.

The vast majority of banks in the CEMAC sub-region have not yet adopted pre-paid cards for the products they offer to their customers, and thus continue to offer debit cards only, whose growth is proportional to beneficiaries' bank account ownership rate.

The case of the bank Crédit du Congo is indicative of this trend.

Over the last ten years, the bank has issued an average of 26,729 debit cards per year. Between 2004 and 2013, the annual number of cards issued was relatively stable. These figures reached their peak in 2014, when the number of pre-paid cards issued grew by almost 25%, totalling 33,397.

Unlike debit cards, pre-paid cards are not linked to a bank account.

In the CEMAC area, pre-paid cards are electronic payment instruments within the meaning set out by Regulation 01/11-CEMAC/UMAC/CM of 18 September 2011. This refers to a set of *"signals recorded in a computer memory included in a personal card provided by an issuer to a cardholder*[11]". Both the boom in information and communication technology (ICT)—principally telephony—and developing countries' clear desire to reduce financial exclusion have encouraged the development and expansion of the pre-paid card offering.

Pre-paid cards work like traditional debit cards. Cardholders can only make payments and/or withdrawals up to the monetary value stored on the card. However, unlike a debit card, owning a pre-paid card is not subject to bank account ownership. Nonetheless, pre-paid cards are linked to an e-money account or e-money wallet, and can only be issued by an institution that has received express authorisation to do so. In Central Africa, only credit institutions are permitted to issue e-money.

As with an e-money wallet, cardholders must load the card with a certain amount of money. Every time a purchase or withdrawal is made, the amounts and any associated fees are deducted from the balance. When the balance falls to zero, the cardholder must reload the card in order to carry out new transactions. Pre-paid cards are used by almost all population segments: those who do not have bank accounts, those who have banking suspensions, young people who have not reached the age of majority, travellers, and even bank account holders who do not want to provide their bank details.

Additionally, other features can be linked to a pre-paid card, depending on the issuer. Some of these services include money transfer (card-to-card and fund

11 Regulation 01/11-CEMAC/UMAC/CM on the conditions for exercising the activity of issuing e-money, article 1.

releases), paying bills, or purchasing mobile telephone airtime. On the Cameroon banking market, some banks that issue e-money even offer businesses the ability to pay the salaries of employees who do not have bank accounts directly to a pre-paid card created for this purpose. All of these features are available only via a dedicated platform using specific technologies, most of which are affiliated to the international networks Visa and MasterCard. The software and physical infrastructure varies based on the pre-paid solution used by the issuing institution.

Pre-paid cards offer several advantages, and first and foremost are an alternative to a bank account. They allow their holders to receive basic financial services (make withdrawals and payments, view their balance) and to store their money more safely. They are also a driver of financial inclusion as they allow those who are excluded from the formal financial system to gain access to certain financial products or services. Finally, they increase the speed and security of financial and commercial transactions.

Although the advantages and benefits of pre-paid cards are undeniable, their existence may promote misconduct contrary to the laws and regulations set out by CEMAC member states.

2.4.1.1 Distribution of pre-paid bank cards

A large number of banks in the sub-region do not offer pre-paid bank cards. For example, of the 13 banks operating in Cameroon, only Ecobank Cameroun, Afriland First Bank, Atlantique Bank and UBA Cameroun issue this type of NPM.

Based on results from the detailed semi-directive interviews, it emerges that card distribution involves the plastic card manufacturer, a card customising company, a service provider, the bank and the customer. Banks and sometimes MFIs are card issuers and acquirers. They carry out data routing and ensure that these instruments are connected to ATMs and EPTs. They also perform transaction clearing and archiving.

In principle[12], customers visit bank staff at the counter to obtain a pre-paid card. Before being given a card, customers must fill out a registration form and provide proof of identification. Card personalisation takes place after it has been confirmed that the customer is not on the bank's blacklist and the registration contract is signed by the manager.

In the banks that were studied, e-money flows linked to the use of pre-paid

12 Some credit institutions allow their ATMs to issue pre-paid cards

cards converge at the provider's localised platform (e.g.: Atos Cardamone). The provider acts as an intermediary between card issuers and the bank in terms of flows of e-money. In addition, ATMs are linked to the provider's payment platform, which clears the flows of money.

2.4.1.2 Demand for pre-paid bank cards in the CEMAC region

To be able to use pre-paid cards, their holders must have a supply of monetary units. Regulations set caps on the value of cash withdrawals and payments that can be made. These regulatory ceilings are summarised in the table below:

Table 1: NPM transaction caps

REFERENCE	DESCRIPTOR	NORM OR STANDARD (In CFA francs)[13]
REM CP1	Electronic instrument cap	5 000 000 FCFA
REM CP2	Daily loading cap (cash)	2 000 000 FCFA
REM CP12	Daily loading cap (bank transfer)	5 000 000 FCFA
REM CP3	Withdrawal cap per transaction (manual or ATM)	500 000 FCFA
REM CP4	Cap per transfer	1 000 000 FCFA
REM CP5	Cap per payment	1 000 000 FCFA
REM CP6	Daily withdrawal cap	750 000 FCFA
REM CP7	Daily transfer cap	1 500 000 FCFA
REM CP8	Daily payment cap	2 500 000 FCFA
REM CP9	Daily transaction cap (withdrawals + transfers + payments)	3 000 000 FCFA
REM CP10	Weekly transaction cap (withdrawals + transfers + payments)	5 000 000 FCFA
REM CP11	Monthly transaction cap (withdrawals + transfers + payments)	10 000 000 FCFA

Source : BEAC

13 One euro = 655.96 CFA francs

The surveys revealed that within the CEMAC, individuals are the main parties that request pre-paid cards. These are principally used to withdraw money from ATMs and to make payments via retailers' EPTs. In banks, pre-paid cards are reloaded either with cash in banks or by debiting a bank account. They can also be reloaded via the bank's website by debiting the customer's bank account.

The information available on pre-paid cards was collected from [14]:

- UBA, Afriland First Bank in Cameroon;
- UBA in Gabon;
- UBA in the Congo

However, only the banks operating in Cameroon provided sufficiently detailed information.

Year-on-year figures show that the number of pre-paid cards issued by Afriland First Bank grew from 12,773 in 2013 to 16,326 in 2014 (an increase of 27.81%) to 20,322 in 2015. Over the same period, at UBA Cameroun, this number grew from 2,555 to 50,050 (an increase of 1859% between 2013 and 2014) and to 145,850 in 2015. The figures reported by Ecobank Cameroun remained relatively stable.

Year-on-year figures at Afriland First Bank also show that the number of active pre-paid cards represents, on average, 96.9% of the total number of cards. The value of the transactions made via these cards rose from 4,385,700,062 CFA francs (€6,685,926) to 4,718,154,598 CFA francs (€7,192,750) between 2013 and 2014, an increase of 7.58%. This figure grew to 5,752,463,745 CFA francs (€8,769,534) between 2014 and 2015, a 21.9% increase in relative value.

The value of the transactions made via pre-paid cards issued by UBA Cameroun rose from 56,387,500,000 CFA francs (€85,961,796) in 2013 to 125,125,000,000 CFA francs (€190,750,960) in 2014, an increase of 121.9%. Between 2014 and 2015, the value of these transactions increased by 45.7% to 182,312,500,000 (€277,932,343).

At Ecobank, between 2013 and 2014, the value of these transactions increased from 105,132,292,000 CFA francs (€160,272,412) to 178,006,239,000 CFA francs (€271,367,520), an increase of 69.31%. Between 2014 and 2015, the value of these transactions increased by 7.15% to 190,735,811,000 (€290,773,540). Across all of these banks, it is clear that the volume of activity linked to pre-paid cards is increasing over time.

Table 2: Pre-paid card offerings from several Central African banks

Source: survey data

14 Not all of the banks in the CEMAC area offering pre-paid cards made information relating to this activity available to the working group. In addition, as the BEAC does not have detailed aggregated information on this topic, the statistics presented in this report are only partially representative of the actual situation in the pre-paid card market in the CEMAC area.

Pre-paid card statistics – Afriland First Bank Cameroun

Indicators	2013	2014	2015	2016 (au 30/06/16)
Number of registered pre-paid cards	12 773	16 236	20 322	21970
Number of active pre-paid cards	12 339	15737	19 750	21390
Number of ATMs	61	78	85	102
Number of EPTs	195	208	219	266
Number of transactions made	371 074	385 498	407 347	204 219
Value of transactions made	4 385 700 052	4 718 154 598	5 752 463 745	3 067 926 896
Current balance on pre-paid cards	489 977 408	522 919 184	687 069 366	700 021 527

Pre-paid card statistics – UBA Cameroun

Indicators	2012	2013	2014	2015
Number of registered pre-paid cards	2 555	2 555	50 050	145 850
Number of active pre-paid cards				
Number of ATMs				
Number of EPTs				
Number of transactions made				
Value of transactions made	12 775 000 000	56 387 500 000	125 125 000 000	182 312 500 000
Current balance on pre-paid cards				

Pre-paid card statistics – EcobankCameroun

Indicateurs	2012	2013	2014	2015
Number of registered pre-paid cards	1	7 422	7 321	8 158
Number of active pre-paid cards				
Number of ATMs				
Number of EPTs				
Number of transactions made				
Value of transactions made	3013 000	105 132 292 000	178 006 239 000	190 7 35 811 000
Current balance on pre-paid cards				

Between 2012 and June 2016, the only Cameroonian banks that agreed to provide information—at the insistence of Cameroon's monetary authority and coupled with the threat of sanctions in the event of non-compliance, it must be noted—issued pre-paid bank cards used in transactions with an overall value of 868,401,600,301 CFA francs (€1,323,863,650). Aside from the fact that their projections based on the figures as at 30 June 2016 show transaction values increasing to double the 2015 values, two of the banking ins-

titutions do not show any current balance on pre-paid cards at 31 December in any years.

In the sub-region, the lack of a system providing a general overview of the pre-paid card payment system was a not insignificant obstacle to data collection. There is no entity such as there is in Portugal, where there is an entity that manages all DABs. In addition, there is no centralised card reference framework listing the name of card users and card numbers, etc. From interviews with various stakeholders, it appears that management of flows from pre-paid card transactions is not a priority for the sub-regional regulatory and monitoring authorities, one of whose assigned tasks is, it should be remembered, to ensure financial and monetary stability in the sub-region.

2.4.2 Mobile money

For the majority of the institutions with mobile money offerings, this payment method was introduced to the sub-region after 2010. Mobile money allows users to make transactions through a system of monetary units using mobile telephones. Mobile money transactions require an electronic account to be opened. Approval to offer mobile money products is granted financial institution which partners with mobile telephone operators. by a partner bank, which creates a guarantee fund that covers all of the e-money. The financial institution or partner bank issues electronic money through an account in its books that holds the scriptural equivalence of all virtual money in circulation. As such, banks are the issuers of mobile money. In the CEMAC, the following mobile money products are offered:

National payments: money transfers between two people living in the same country (also called P2P).

Money storage: in certain systems, the account is used to store money securely, whether through an account opened with a bank or, more commonly, an account opened with a mobile operator.

Retail payments: payments to participating retailers. These retailers can be supermarkets, consumer goods retailers, or the mobile operator itself (for users to purchase airtime for making calls or other services).

Payment for bills or other services: for paying bills for essential services such as water and electricity in a convenient and effective way, paying for school costs, taxes, etc.

Table 3: List of credit institutions in the CEMAC authorised to issue mobile money

Country	Issuer	Technical operator	Product type	Authorisation date
Cameroon	BICEC	Orange	Mobile Money	29/07/2011
	ECOBANK	MTN	Mobile Money	29/07/2011
	Afriland First Bank	MTN	Mobile Money	29/07/2011
	SGC		Mobile Money	02/12/2011
TOTAL		4		
Congo	ECOBANK	MTN	Mobile Money	29/07/2011
	BGFI BANK	Airtel	Mobile Money	03/10/2011
TOTAL		2		
Gabon	BGFI BANK	Airtel	Mobile Money	29/07/2011
	BICIG		Mobile Money	11/07/2012
	ORABANK	Atlantique Téle-coms (Moov)	Mobile Money	
	UGB	Gabon Telecom	Mobile Money	20/01/2014
TOTAL		4		
Tchad	ECOBANK	Airtel	Mobile Money	05/03/2012
	ORABANK	TIGO	Mobile Money	11/07/2012
TOTAL		2		
OVERALL TOTAL		12		

Source : BEAC

When reading this table, it can be seen that of the approximately fifty banks operating in the sub-region, only twelve have received approval to issue mobile money. Of the banks that have received approval, some, such as Société Générale or Ecobank in Cameroon are currently not issuing mobile money.

2.4.2.1 Mobile money distribution

Mobile money is a service that allows customers to make financial transactions using their mobile telephone.

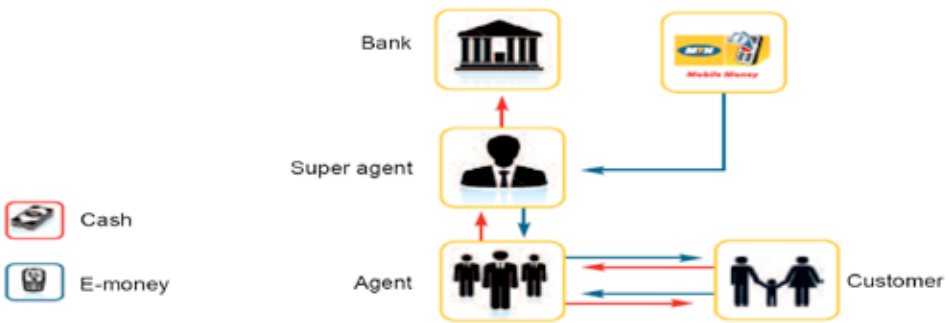
This service is an important tool for financial inclusion. It allows a significant proportion of the unbanked population to become integrated into the banking system.

The BEAC has regulated mobile money by authorising a partnership between banks—the only parties permitted to issue e-money—and mobile telephone operators to make the service accessible to their customers.

The use of mobile money involves a number of stakeholders:

- the bank, which keeps a deposit equal to all of the virtual funds in circulation on the mobile money platform;
- the mobile telephone operator, which is responsible for developing the mobile money network, providing SIM cards to customers, and generally managing the mobile money platform;
- the mobile money agent, who obtains virtual money by depositing the equivalent in physical money with the bank;
- the retailer who receives mobile money payments from customers;
- customers, the end users who credit and debit mobile money accounts across the network of distributors, and are able to carry out mobile money transactions.

The partner bank manages an equivalent sum of money to the total amount circulating in mobile money accounts. It is responsible for and guarantees the issuance of e-money, and ensures that transactions comply with current laws on money laundering and terrorism financing. Banks do not always have their own platform.



The regulator does not have real-time access to the platforms. Nonetheless, the platforms are certified, which ensures reliable account management from the regulator's viewpoint.

However, banks have real-time access to the information on the platforms. Mobile telephone companies manage the transaction platform, including the virtual money. Distributors receive the money created and distribute it. They make deposits in the guarantee fund in order to make mobile money available

to resellers and distribution agents. Distribution agents are linked to distributors and make withdrawals from and deposits into customers' accounts. Acceptors are retailers who accept mobile money payments.

To obtain mobile money, distributors purchase e-money units from mobile telephone operators. Resellers also use distributors. End customers themselves obtain e-money units by paying in cash at resellers' and retailers' points of sale.

For merchants to receive payments via mobile money, they need to fulfil a set of conditions written into a legal document following consideration of their case by an agent of the mobile telephone company and, if required, the signing of a contract between the partner bank and the merchant, with the contract having previously been approved by a partner bank. A retailer account is opened on the mobile telephone operator's management platform and a copy of the contract is sent to the bank to open a retailer account on the platform.

For distributors and acceptors, the documentation includes the taxpayer's card, registration on the trade register, a map, a photo of the manager and proof of address, such as water or electricity bills. Via the platform, the bank has access to a list of distributors and other intermediaries, but not of end customers. As a result, it does not have any trace of the transactions carried out by end customers. Instead, it controls the stock of available e-money.

Mobile money distribution requires a number of pieces of information to be passed on from mobile telephone operators to their partner banks. In particular, this covers the volume of transactions, any fraud, distributors' activities, and compliance with regulations on transaction amounts and caps.

2.4.2.2 Demand for mobile money in the CEMAC

The main users of mobile money are individuals or legal persons, who may or may not have a bank account, and are subscribed to a mobile phone operator. They include people living in suburban and rural areas, retailers and unbanked employees.

Mobile money can be used to withdraw cash as well as to pay bills to retailers, pay taxes and duties, make online payments, purchase items and airtime, and transfer money. Essentially, these are peer-to-peer (P2P)[15] and peer-to-cash (P2C) money transfers. In addition, mobile money encourages savings among unbanked populations or those who live in rural areas, thus contributing to

15 IT network model in which every client is also a server.

financial inclusion. To be able to use mobile money, customers must have a telephone line and fill in a registration form, attaching a copy of their national identity card. The table below features statistics on mobile money in the CEMAC area. Only Airtel in Gabon and MTN and Orange (and their respective partner banks Afriland First Bank and BICEC) in Cameroon provided sufficient information.

As shown in the tables below, and based on information collected from the Cameroon- and Gabon-based operators only, almost 868,702,238,000 CFA francs (€1,324,321,000) was transferred using mobile money between 2011 and the end of June 2016.

Table 4 & 5: Mobile money offerings in Central Africa (source: survey data)
Mobile money statistics—MTN & Orange—Cameroon

Indicators	**2011***	**2012***	**2013**	**2014**	**2015**	**2016** (au 30/06/2016)
Number of registered mobile money accounts		628 378	2 738 901	3 589 086	3 796 051	6 284 061
Number of active mobile money accounts	3 589	68 799	1 442 692	1 738 976	2 172 792	2 808 249
Number of registered agents	659	264	6 849	5 991	17 219	11 952
Number of active agents	206	400	1 969	4 461	4 943	6 379
Value of mobile banking transactions carried out (in thousands)	**372 581**	**7 563 478**	**30 789 734**	**71 993 361**	**201 397 836**	**315 685 248**
Number of mobile banking transactions carried out		998 277	3 273 148	8 951 175	25 096 057	28 907 949
Current balance of bank accounts (in thousands)	20 499	172 039	1 840 056	8 790 596	9 845 234	10 159 347

**statistics relating to the operator Orange Cameroun only*

Mobile money statistics – Airtel – Gabon

Indicators	2 012	2 013	2 014
Number of mobile money accounts	294 428	2 687 540	6 261 740
Value of transactions	12 600 000	76 100 000	152 200 000

In the CEMAC, and in particular in Cameroon, it appears that the use of mobile money became more widespread from 2013. In that year, the number of mobile money accounts registered with technical operators grew to over 2,700,000, and active accounts saw their highest annual growth between 2011 and the end of June 2016—almost 2000%. As expected, the number of

distribution agents increased at a similar rate to the number of mobile money accounts, with a peak in 2013.

In 2016, the total number of accounts surpassed 6,200,000. However, one in three accounts is not active.

In terms of financial flows via mobile money transactions, the annual value has increased by an average of 170% every year since 2013. At the end of June 2016 (1st year half), this value is estimated at over 315 billion CFA francs (57% more than the total value of the previous year).

The slowdown in growth in stock levels (balances) in mobile money accounts confirms that this financial instrument plays a major role as a method of "instant" money transfers between users and highlights the increase in velocity of circulation of the financial flows involved. For example, it can be seen that year-on-year growth figures for balances held with Cameroonian banks using this tool were 970% in 2013 but only 12% in 2015 (and 3% in the first half of 2016). This means that mobile money transfers are carried out in increasingly short timeframes.

In Gabon, the total value of mobile money transactions via the operator Airtel doubled in two years to over 150 billion CFA francs in 2014 and, as in Cameroon, 2013 was a milestone year with growth of over 813% in the number of mobile money accounts opened with Airtel Gabon. In 2014, the total number of accounts was approaching 6,300,000[16].

In summary, based on the institutions considered here, it is clear that demand for mobile money in the CEMAC area has experienced very significant growth in the last three years. In the same vein, the volume of mobile money transactions has undergone a spectacular increase.

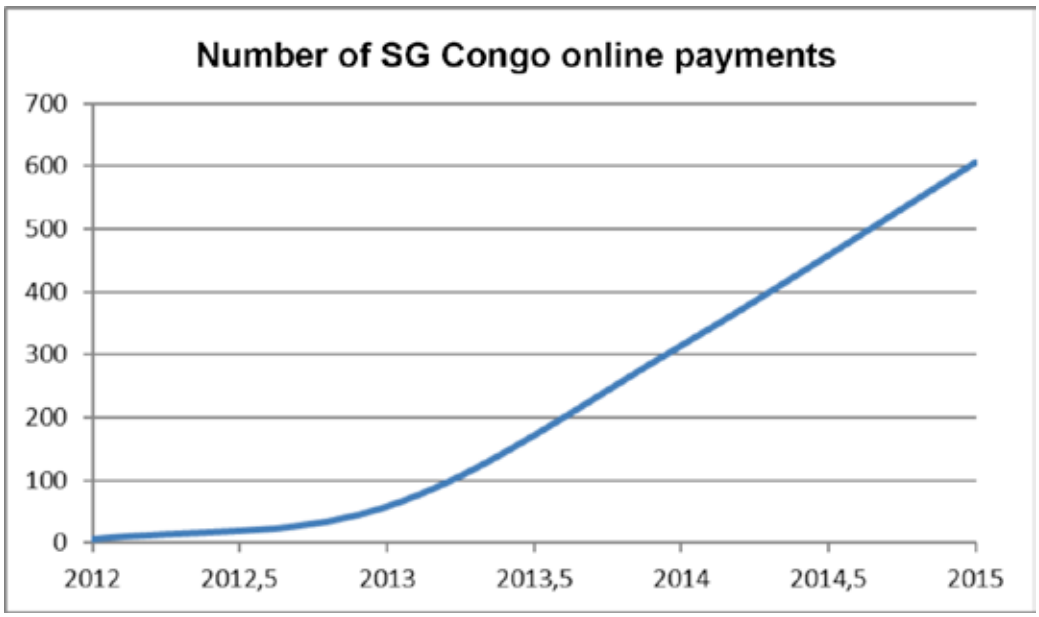
2.4.3 Online payments

Online payments in the CEMAC began in the early 2000s. The main parties involved in online payment offerings are the online payment gateway, websites and banks.

The online payment gateway is the provider of online payment products. To carry out an online payment transaction, a customer space is created on the website where purchases are made. The customer space is authenticated by the internet service provider every time customers attempt to use the site to make a purchase.

16 Considering Gabon's population (1,800,000 inhabitants), the working group believes that the number of accounts stated is due to a failure by the operator in question to update their customer records

Within an organisation such as Société Générale du Congo, although the number of online payments is certainly increasing from year to year, it nonetheless remains low, with 605 online payments in 2015. This growth is represented by the following graph:



To make online payments, customers are required to register with a retailer site, sign a contract, and have a username and password. Customers must also access their own space and hold an electronic wallet or a card linked to an international payment system. Online payments are mainly used for the purchase of goods and services, but some banks offer an online transfer service. The main users of online payments are companies and individuals, the majority of whom have previously travelled abroad.

The NPM offering in the sub-region poses a number of technical, monitoring and regulatory problems. Technical problems are linked to network instability. Monitoring problems are due to banks' poor monitoring of the NPM activities provided by their partners. Information on banks' partners' activities is not always comprehensive and/or available in real time. Checks on users' identities and the origins of funds are not always carried out, and regulatory caps are not always obeyed. In addition, monetary authorities' regulation and monitoring of NPM offerings is ineffective ■

CHAPTER III

Risks of money laundering and terrorism financing via new payment methods in the CEMAC

Both the boom in information and communication technology (ICT)—principally telephony—and the clear desire of the sub-region's countries to reduce financial exclusion have encouraged the development and expansion of new payment instruments, such as pre-paid cards and mobile money. Although the advantages and benefits of pre-paid cards are undeniable, their existence may promote misconduct contrary to the laws and regulations set out by CEMAC member states.

However, the research team noted that the risks of money laundering and terrorism financing resulting from the use of new payment methods are poorly understood by various stakeholders in the chain, and that these parties, although they are trained in and made aware of the due diligence to which they are subject vis-à-vis their customers when carrying out their transactions, are not informed of the ways in which offenders of all kinds may misuse these NPMs.

The seminar organised by the GABAC at the time this typologies exercise was launched (during which several specialists from a range of backgrounds and professions from the field gave presentations on the theme of NPMs) and the interviews and working sessions that the working group organised throughout the exercise led to the identification of a number of NPM-specific vulnerabilities to money laundering and terrorism financing in Central Africa. As consumer habits in the sub-region mean that online product sales are very limited, we will only discuss the risks of or vulnerabilities to money laundering and terrorism financing that are linked to the use of pre-paid cards and mobile money.

3.1 Risks common to all new payment methods

3.1.1 Risks linked to weaknesses in the regulatory system

Although introduced relatively recently, regulations on the practice of issuing e-money and the use of NPMs seem to take into account possible misconduct that could lead to money laundering and terrorism financing. However, some regulatory lacunae nonetheless remain, and these could facilitate the occur-

rence of such phenomena. The regulations governing the use of NPMs in the CEMAC area are somewhat silent regarding the combating of money laundering and terrorism financing (Ndjimba, 2016), particularly on the following aspects:

- the lack of regulatory provisions specific to NPMs and to controlling the risks that may arise from their use;
- checks on the origins of funds deposited in return for the issuuance of e-money, on the purpose of transactions, and on the destination of funds. Provisions of this order would improve transaction traceability;
- real-time transaction monitoring with the aim of reducing the risks linked to the speed at which e-money circulates via NPMs;
- the caps on transaction volumes, which remain too high and seem to have been set without taking into account the possible fragmentary nature of these transactions or the possible use of smurfing; supervision of new market stakeholders, particularly those involved in the mobile money distribution circuit. This circuit can present a number of vulnerabilities linked to the low levels of training given to agents and distributors, who are often not financial sector professionals, to the way in which NPMs are used, and to the regulations and other mechanisms designed to prevent ML/TF risks arising from the use of NPMs.

In addition to these regulatory weakness regarding the use of NPMs for money laundering or terrorism financing purposes, there is also the issue of limitations due to risk factors regarding the way e-money is issued and the NPMs through which it is used.

3.1.2 Risks linked to the range of stakeholders and the speed of technological developments

The working group agrees with the following general statement [17]: "The risks inherent to e-money also come from those connected to the various players involved in issuing, managing and distributing these products, as well as from the rapid rate of technological change, which very often outpaces public authorities' ability to adapt.

For example, five categories of stakeholders operate in the pre-paid card value chain:

17 Source: TRACFIN study, Monnaies électronique, monnaies virtuelles et nouveaux risques [Electronic currencies, virtual currencies and new risks]

- The card issuer, who is approved by a supervising authority and is responsible to this authority. The issuer is also responsible for ensuring that users can use the card properly. The pre-paid card is the format in which the e-money is stored;
- The network (MASTERCARD, VISA, AMERICAN EXPRESS, JCB-CUP, etc.), which manages transaction authorisations. Belonging to a network allows the card to be accepted at points of sale affiliated to that network;
- The processor, which manages the technological and computing aspects of the card;
- The programme manager, which deals with all non technological matters: marketing, packaging, compliance, logistics, the practical management of the product, and customer services. Banks, specialist market stakeholders, bureaux de change, small companies, etc. may act as programme managers;
- The distributor, who markets the card and interacts directly with customers (newsagents, retail chains, local shops, etc.).

Transactions are identified by the network, the processor and the issuer. The card issuer also retains card numbers in its systems (authorisation servers) for any future searches. These three operators can distinguish transactions made using a pre-paid card from those made using a traditional bank card. Upon issuing the card, it is linked to a BIN, a bank identification number featuring a key that can be used to determine whether a given card is a pre-paid card, a company card or an individual card. It appears that although the issuer is legally responsible for diligence efforts as regards money laundering, the key aspects of "Know Your Customer" can only be collected through the programme manager and the distributor.

In addition, stakeholders in the e-money sector—particularly distributors—are from a non-banking background whose know-how and experience of KYC is more limited than in the traditional financial sector.

The networks through which these new payment methods are distributed are often non-financial operators with little knowledge of the combat against money laundering and terrorism financing and who may even be reluctant to introduce diligence measures, which can be seen as an expensive obstacle to distributing the products in question.

Thus the working group learned that Orange Cameroun, although supervised by BICEC, issues electronic money via its "Orange money visa card" without neither due authorisation nor evaluation by BEAC or GIMAC the risk of money laundering and terrorism financing inherent to the product.
Another factor that increases the risk of failings is the fact that the market is

developing quickly and has not yet stabilised. As a result, institutions are in fierce competition with each other and are using increasingly inventive means to boost their turnover.

Given the risks of technological developments, it should be remembered that FATF Recommendation 15 states that: "Countries and financial institutions should identify and assess the money laundering or terrorist financing risks that may arise in relation to (a) the development of new products and new business practices, including new delivery mechanisms, and (b) the use of new or developing technologies for both new and pre-existing products. In the case of financial institutions, such a risk assessment should take place prior to the launch of the new products, business practices or the use of new or developing technologies. They should take appropriate measures to manage and mitigate those risks." As a result, issuers of e-money who are entering the field of financial institutions must be able to propose products and monitoring procedures that reduce the risk. However, this obligation is not obeyed given the particularly competitive nature of the sector.

[In Central Africa, it is generally recognised that no assessment of the risk of money laundering or terrorism financing linked to NPM offerings was carried out before they were placed on the market.] Technological developments are tending towards increasingly quick transactions, often faster than more traditional networks, whether in the speed of loading or unloading these new payment methods, but also in terms of the distinction between purchasing a card/creating an account and the ability to load a card at a later date, transfer funds, etc. by simply sending an SMS message or clicking a button online. The speed of these flows can also make monitoring significantly more difficult and can prevent the seizure and freezing of assets of criminal origin. The chain of information is more complex than in a traditional banking circuit—for the same financial transaction, analysis of the flow means calling on a wider number of contacts, some of whom are located outside of the CEMAC's jurisdiction. As a result, the investigative process is slowed down."

Repeated attacks from cybercriminals, to which a Gabonese bank and one of its branches in Congo had fallen victim, substantiates the above.

3.2 Risks linked to prepaid cards

3.2.1 Banks' opacity

All banking institutions in the sub-region were invited to take part in the typologies exercise that is the subject of this report. However, only those representing major international groups and a Cameroonian bank agreed to

participate. Nonetheless, firstly, the major groups do not offer a pre-paid card service, and the value of the transactions by the Cameroonian bank represents only 1.72% of the sample studied. Secondly, members of the working group learned that the credit institutions that did not agree to take part in this exercise are reportedly involved in investigations into large-scale funds transfers to West African countries affected by terrorism and into manual foreign exchange transactions on behalf of individuals who are involved in money laundering in the countries in which they are located. They also exceed the caps on loading pre-paid cards with funds.

3.2.2 Cardholder anonymity

Pre-paid cards can be issued in a particular cardholder's name or anonymously depending on available options. Generally, cards are sold to occasional customers [18] who are not consistently identified, and who pay for their purchase and load the card using cash. Cards can be purchased from banking institutions[19] or from e-money distributors[20].

As the same card features are common to all cards, in principle, anonymous cardholders enjoy the same services as cardholders who have been identified via the standard process. However, without formal identification, institutions and distributors are not capable of determining the cardholder's identity or the origin of the funds used to purchase and load the card. In other words, a customer with money of suspicious origin or originating from illegal activities can easily incorporate the proceeds of their crime into the formal financial system via one or several pre-paid cards. Anonymous card ownership is therefore a gap through which criminals and mafia-style organisations of all kinds can easily slip.

3.2.3 Failure to comply with the caps set out by the BEAC

The caps on loading, withdrawals, payments and transfers and on each transaction, which suggest that the availability of pre-paid cards has been hijacked from its purpose of financial inclusion, can result in misuse of all kinds in light of the statistics presented above.

This is particularly true when these caps are very large and can benefit anonymous cardholders. Currently, pre-paid card loading caps may be as high as

18 "An individual or corporation with no account with the institution to which the request was made", COBAC Regulation R-2005/01 on due diligence procedures for institutions governed by rules to prevent money laundering and terrorism financing in Central Africa.

19 An institution that is authorised to issue e-money.

20 An institution offering the holder of the electronic instrument an e-money loading, reloading and cashing service following the signing of a contract with a banking institution.

10 million CFA francs (€15,245) per month in Cameroon[21] and 25 million CFA francs (€38,115) per week at one bank in Gabon. The same caps apply to ATM withdrawals and payments.

Although institutions set these caps to suit a range of market segments, the majority nonetheless remain very high, especially for withdrawals. This also does not take into account the fact that, as there is no centralised system holding information on pre-paid card transactions, a customer (whether a bank account holder or not) can, in full compliance with each bank's regulatory caps, circumvent the limits set by each account by repeatedly loading money onto a card in as many banks as required, whether in the customer's home country or in the sub-region.

3.2.4 Risks of laundering the proceeds of tax and customs fraud

In the sub-region, pre-paid cards are primarily used by operators for international business purposes. This includes importers, for whom, it must be said, tax compliance is not a major concern. As such, as for debit cards, pre-paid cards give them the ability not just to circumvent community exchange regulations but also to reduce the values declared to customs, thus reducing the relevant taxes and duties. This practice also reduces the taxable base for any internal taxes for which they are liable. The fraudulently gained profits are then invested in a range of sectors (property, large-scale agricultural projects, oil product distribution, etc.).

Although this is not the aim of this study, we do want to draw the attention of monetary authorities to the fact that, in addition to the lost fiscal revenue that results and the deficit in the trade balance in which the practice plays a major role, the use of pre-paid cards in external trade could be one—and not the least—of the unexplained causes of the fall in currency hedging financial transactions, not to mention the loss of tax that may have been due on commissions taken by banks on transactions carried out by their customers outside the CFA franc area.

3.2.5 Money laundering through the circumvention of automatic declaration thresholds

The majority of the countries in the sub-region have enacted legislation that, under certain conditions, requires financial institutions to automatically declare all cash deposits of 5,000,000 CFA francs (around €7,625) to financial intelligence units. As part of the first step in money laundering (placement), operators can load their pre-paid cards in a number of transactions, with each

21 Competitive monitoring

transaction's value being less than the automatic declaration thresholds. This introduces money into the financial system that may come from, for example, corruption and/or misappropriation of funds, drug dealing, illegal sales of precious gems and metals, or any other proceeds of crime.

3.2.6 Risks linked to carrying out transactions

Control of e-money flows is the main risk factor when transactions are carried out via NPMs. In the sub-region, banks have no control over their payment platforms, which are located outside the jurisdiction in which they operate. This can result in information on the transactions carried out using pre-paid cards via the supplier's services being manipulated, facilitating suspicious transactions. In addition, the quality of the internet connection can lead to transactions being carried out without being subjected to real-time analysis.

Furthermore, insufficient or non-existent training for banking staff on the computer systems responsible for pre-paid cards and on money laundering regulations and techniques may facilitate suspicious transactions due to human error. Thus, when faced with signs of a transaction that is part of a money laundering or terrorism financing operation, an agent who has not received sufficient training or any training on the topic will not be able to identify the suspicious nature of the transactions and thus will not make the necessary declaration of suspicion as required by law, unless there is a centralised monitoring system that can detect suspicious transactions that were not detected at the first point of vigilance.

This is a major operational risk, particularly when monitoring bodies do not carry out regular checks on transactions. This risk is made all the greater by the fact that in these institutions, there is no electronic alert system that identifies signs of suspected money laundering or terrorism financing. The use of a manual system to check transactions for these signs thus reveals itself to be very limited. This method is prone to errors and to agents' inability to detect all signs, given the considerable volume of transactions to be analysed.

The lack of a computerised analysis system may constitute a weakness in the transaction management system when identifying suspicious transactions.

Faced with these multiple risk factors that exist at both an organisational and a systemic level, it is essential that a systematic approach to preventing the risks of money laundering and terrorism financing is put in place.

3.2.7 Laundering cybercrime proceeds and financing terrorism with cybercrime proceeds

Proceeds from the following methods of fraud can be used for money laundering and/or terrorism financing.

These include:

Physical fraud. This includes, but is not limited to:

- fraud linked to counterfeiting pre-paid cards that imitate real cards both in terms of appearance and content, to "yes cards", counterfeiting chip cards that respond OK to all secret codes entered;
- counterfeiting terminals using data collection techniques such as modifying terminal data to extort sensitive data.

Online fraud. This consists of:

- redirecting the IP address without the web user's knowledge;
- website phishing;
- Stealing data from the computer systems of banks, processors or retailers;
- Attacking the issuer's computer database by intercepting nodes, accessing servers, decrypting messages, etc.

3.3 Risks linked to mobile money payments

Mobile money services are currently being rolled out in a number of markets around the world. There is concrete evidence to suggest that these services improve access to formal financial services in developing countries.

However, the expansion of these services arouses fears that they may be used for the purposes of money laundering and terrorism financing (ML/TF). Although there have been very few cases of ML/TF up until now, mobile money systems remain susceptible to being used for these purposes in the future (in the same way that other formal financial services are currently being targeted)
.
The risks of money laundering and terrorism financing linked to mobile money transactions are mainly due to failings in the management systems implemented by financial institutions and their respective partners for these instruments. These risks can be classified into two groups: those linked to customer identification and those linked to carrying out transactions at each link in the chain of stakeholders.

3.3.1 Risks linked to customer identification

3.3.1.1 Risks linked to the authenticity of identity documents

The risk of money laundering and terrorism financing is increased in the sub-region in that individuals can easily use false identity documents. The lack of an effective mechanism for mobile telephone operators to verify the authenticity of identity documents is a major obstacle to the prevention of these risks, especially because for many mobile money operators, mobile money can be used after the customer is identified, not after the authenticity of the identity document has been verified. In these organisations, it is often the case that a copy of the identity document is presented, thus rendering it impossible to verify the authenticity of the original identity document. As such, the ability for individuals to move from one country to another in the absence of a sub-regional database for identifying individuals may increase the chance of these risks occurring. The free movement of people between the countries of the sub-region would appear to constitute a risk factor.

3.3.1.2 Risks of money laundering and terrorism financing linked to customers

This risk may arise in the form of a traditional transfer with a criminal origin or destination (for example, financing terrorism). Although real documentary proof may be used at the time of registration, false information may also be presented. The act of depositing money into the account can also be used to recycle fraudulently obtained funds via the use of stolen bank cards or credit cards (which can be considered to be a 'placement' process). Transactions can also be used to transfer funds between accomplices, or to transfer them to other countries with less stringent AML/CTF laws, where the funds can be used to finance other criminal activities. This process is accompanied by cash withdrawal of the amounts to be used or transferred by other methods.

3.3.2 Risks linked to carrying out transactions

3.3.2.1 Risks linked to retailers

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

3.3.2.2 Risks linked to agents, intermediaries and retail partners

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

3.3.2.3 Risks from cross-border payments

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

3.3.3.4 Risks of money laundering and terrorism financing circumvention via international transfers

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

CHAPTER IV

Typologies of risks of money laundering and terrorism financing linked to new payment methods

The combined risks of money laundering and terrorism financing, mentioned above, have led to several typological cases of money laundering and terrorism financing being observed to take place via new payment methods. After presenting these cases, this report features proposals to reduce the risk of ML/TF.

Cases of money laundering and terrorism financing via new payment methods in the CEMAC

From surveys of NAFIs, two known typological cases of money laundering were identified[22]. The first case involved computer fraud relating to pre-paid cards, resulting in money laundering.

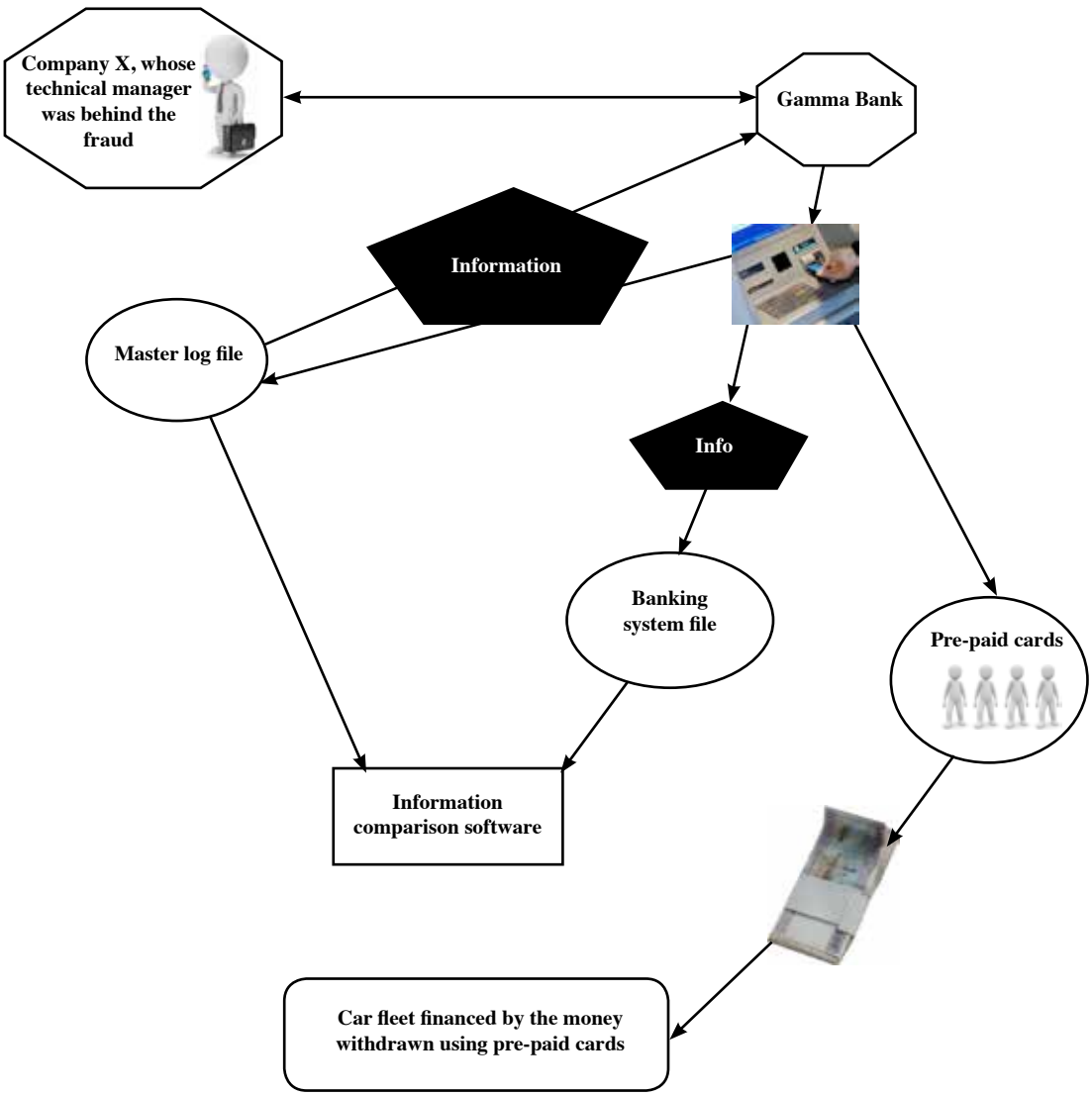
CASE 1: Pre-paid card computer fraud and money laundering

Company X, a specialist in payment system solutions whose CEO is named Mr Pippo, is in charge of managing the electronic payment system at Gamma Bank. As such, it hosts and manages Gamma Bank's electronic payment system servers. On 12 January 2015, Mr Pippo was spoken to by Gamma Bank's managers because transactions seemed to be recorded in their banking system but not in the payment system. Through the combined work of IT technicians from company X and Gamma Bank, it was determined that cash was withdrawn from Gamma Bank's ATMs using 12 pre-paid magnetic cards belonging to 12 individuals. These 12 individuals, each holding a pre-paid card from Gamma Bank, had made repeated cash withdrawals from ATMs. After each transaction, the head of X's technical department, Mr Gando, had connected to the main log file by increasing his privileges so he could alter and remove all traces of the transactions in the activity report of the ATM from which the 12 people in question had made withdrawals. Aware of the delays between updating the payment system and updating the banking system, he deleted information regarding the cash withdrawals carried out by his agents using these 12 bank cards to prevent the banking system from debiting the amounts withdrawn from the relevant accounts. One of the people making these withdrawals repeated the transaction so frequently that he deprived Gamma Bank of 39,000,000 CFA francs over the course of 2014 and 2015.

However, Gamma Bank had implemented an IT solution designed to compare the information contained in the banking system's log file with the payment system's log file at a given moment. This application produced an error report highlighting discrepancies in the information due to certain data being deleted from the payment system's master table. Following analysis of the error report, it became clear that 12 'pre-paid credit' accounts were not

22 Typological cases of money laundering via NPMs, which are highly likely in the CEMAC area given the risk factors identified above, have been identified in the French context (Tracfin 2011, case 5 and 6, pp. 18-23).

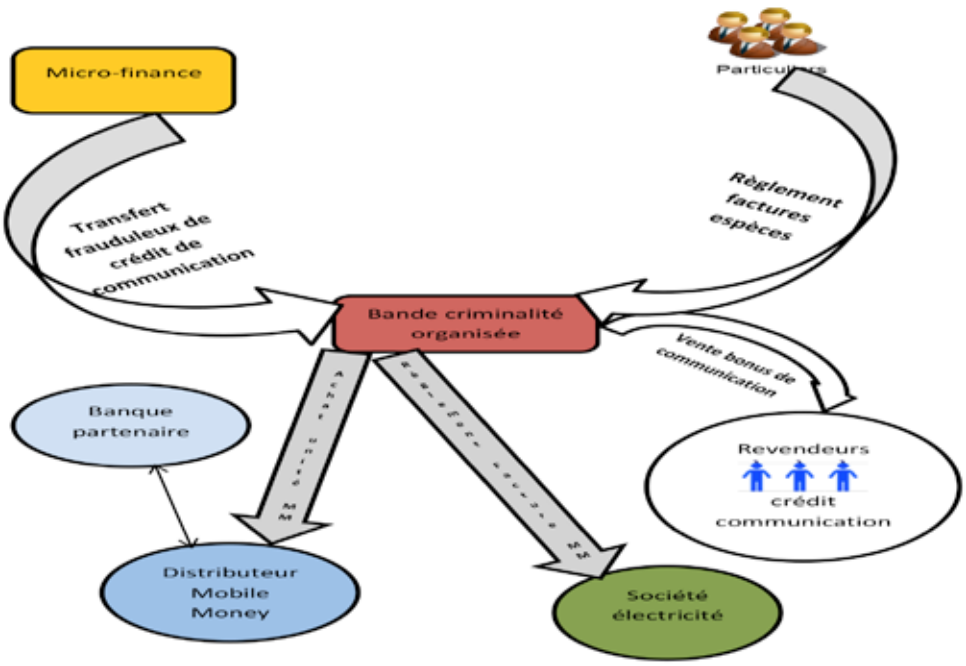
regularly debited despite making withdrawals. Gamma Bank thus contacted the CEO of company X, who in turn contacted Alexander, the India-based supplier and technical manager for Africa for the payment system that X distributes in Cameroon. Alexander checked X's payment system and confirmed to Mr Pippo that the deletion of information from the payment system's master table had taken place within the company itself. During the judicial investigation, Mr Gando accepted the truth before declaring a second-hand car business, which was funded by the embezzled money.



CASE 2: Money laundering via mobile money

After being convicted for fraud, the gang led by Ahomo continued to make a name for themselves by running another form of scam from prison. On 30 May 2014, Mr Bodo, an employee at a microfinance institution, contacted the Public Prosecutor's office to report a scam to which he had fallen victim. The scammers had imitated his boss's voice to ask him to make credit transfers worth 900,000 CFA francs. After he made the transfers to specific telephone numbers, the fraudsters ceased all communication with their victim. Tracing the transactions revealed that the transfers were used to pay several individuals' electricity bills using mobile money, a service offered by a local mobile telephone operator. Following questioning of Mr Abondo, it was revealed that in his neighbourhood in Bantoma, two young people who claimed to be employed by the electricity company had offered locals the ability to pay their electricity bills without having to queue at the company's registered branches.

On several occasions, several residents gave these fake agents their bill along with sufficient cash to pay the bill and taxi fares. He added that after each transaction, genuine payment receipts for their bills were returned to them. In addition, after every bill paid using mobile money, the mobile telephone operator granted the subscriber an airtime bonus. These fake agents then sold this airtime to airtime resellers, known as "callboxers", at tempting prices. Ultimately, the cash received from the population and the callboxers was returned to Ahomo's gang, whose members were still in prison.



CASE 3: Cybercrime, a global phenomenon[23]

Recent cyber attacks show a trend that the targets chosen by the hackers not limited to a specific country rather effects the global financial system.

Latest fraud activity through the use of secured SWIFT gateway, hackers managed to obtain valid credentials of SWIFT operators unlawfully and were successful to hack USD 81 millions of Bangladesh Bank (BB) foreign exchange reserves maintained with FRBNY.

What did intruders do?

- Disabled the Printer linked to the Production Server
- Processed 70 successful transactions through the SWIFT (5 got paid-out)
- Cleaned up several files including message records
- Total 116 messages were deleted – 70 PIs & 46 ACK MSG
- Windows log files were deleted and other files were over written after replacing those files containing garbage data
- Resets the security measures: "firewall" rules back to normal settings
- Correspondence with Intermediary banks like Wells Fargo, Bank of New York, Mellon, Citi NA, DBTCO and PABC
- Two Member IT Team engaged for In-house incident reporting (08th Feb, 2016)
- Appointed World Informatix Cyber Security for detailed incident reporting and vulnerability assessment as part of the investigation (28th Feb, 2016)
- Appointed Mandiant (FireEye) to perform forensic investigation (6th Mar, 2016)
- World Bank assistance sought for recovery of the stolen money under the specific program
- Engaged a Law firm with international exposure to assess legal grounds for recovery of the stolen money
- Informed BFIU and involved BFIU in the recovery process

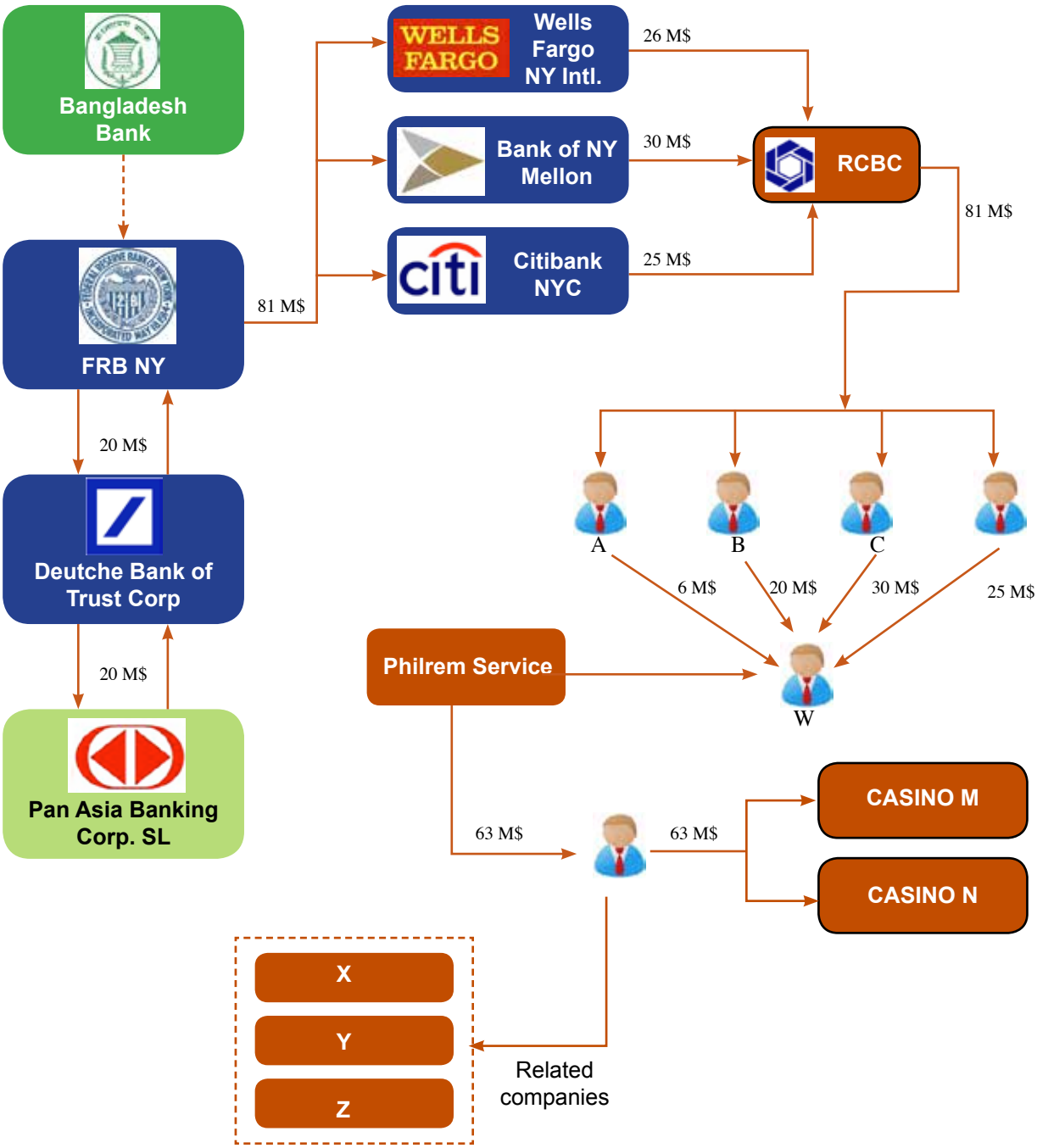
Role of BFIU

- BFIU plays pivotal role to strengthen domestic and international cooperation
- Facilitate formation of the Task Force for coordinating the stolen money recovery efforts (12th Apr, 2016)
- AGO prepared MLA request in consultation with BFIU and sent it to Department of Justice, Philippines under Palermo Convention.(4th May, 2016)
- BFIU sought information regarding suspected persons and entities of Philippines from the Egmont members (15th Mar, 2016) and in some cases received positive responses.
- BFIU continued to pursue AMLC, Philippines
- AMLC obtained court order to seize identified suspected accounts and also to start formal investigation (1st Mar, 2016)
- BFIU maintained communication with FATF and APGML
- BFIU officials involved with the process physically in the Philippines and also attended the Blue Ribbon Senate Committee Hearing
- Tri Party (BB, FRB NY and SWIFT) meeting and teleconference
- Case coordination meeting organized by Interpol and National Counter Terrorism Bureau-Bangladesh

All these actions made the recovery of USD 35 millions possible

23 Courtesy Bangladesh FIU

The money track



CHAPTER V

Recommendations to reduce the risks of money laundering and terrorism financing linked to new payment methods

Recommendations designed to improve the way in which NPMs are managed in the sub-region could include proposals for monitoring and regulating the supply of these financial instruments and for the technical management systems for transactions carried out via NPMs.

These proposals mainly involve:

- improvements to the regulations and supervision governing NPM offerings;
- coordination of activities between those parties that are involved in carrying out this practice by establishing automatic systems for sharing information between issuing companies on transactions that take place via e-money to facilitate the collection of information required by investigations, as well as to detect suspect transactions and declare them to financial intelligence units and to make reports to sub-regional and national supervisory and monitoring bodies;
- capacity building for various stakeholders regarding the issue of money laundering and terrorism financing in general, but also the risks of money laundering and terrorism financing linked to this specific area.

5.1 Improving the regulatory framework for the regulation and supervision of NPM offerings

The various risks listed in this report, including, on the one hand, those linked to cardholder anonymity, pre-paid card caps, laundering of proceeds from tax and customs fraud and the opacity of banks, and, on the other, the difficulty of obtaining aggregated statistics despite the provisions of instruction GR/01 on the monitoring of e-money payment systems by the BEAC are essentially down to regulatory weakness and the reluctance of regulatory, supervisory and monitoring authorities to implement effective measures to structure and monitor NPM-related activities, both at the regional and national level.

In an environment where transactions are inexorably moving to the digital sphere, these these observes weakness do not allow money supply aggregates to be accurately determined, thus preventing the implementation of appropriate measures to secure monetary and financial stability, and they also

prevent effective measures against money laundering and terrorism financing.

In addition to these regulatory weakness, although it is the COBAC's duty, as set out in instruction GR/01, to clarify regulations governing credit institutions to prevent money laundering and counter the financing of terrorism in relation to new payment methods, it has not as yet set out any guidelines or other document establishing NPM-specific due diligence practices that stakeholders should implement in their dealings with technical partners and with their customers.

In any case, it is our opinion that, if the FATF's Recommendation 15 (given above, see section 3.1.2) has not already been implemented, the relevant authorities must improve the legal framework surrounding these new payment methods to minimise their intrinsic vulnerability to money laundering and terrorism financing.

This new legal framework would include provisions that:

1. set out the role and operational responsibilities of each stakeholder involved in e-money activities (regulatory authorities, issuers, distributors, etc.), both individually and in their business relationships;

2. establish the various stakeholders' responsibilities regarding anti-money laundering and counter-terrorism financing;

3. require that a technical system is put in place, including a specific audit trail to ensure that transactions can be traced from the point payment requests are made up until they are concluded. By making the information in this trail easier to collect, it would be an additional source of information during searches following declarations of suspicion and, more generally, for investigations by criminal prosecution authorities;

4. ensure that e-money transactions carried out as part of foreign trade with non-members of the CEMAC area comply with the sub-region's currency exchange regulations;

5. cap e-money holdings to an amount that is compatible both with financial inclusion policies and with the risks of money laundering and terrorism financing that is intrinsic to this form of money. In West Africa, for example, without special permission from the Central Bank, e-money holdings cannot exceed 2,000,000 CFA francs (around €3,000), and similarly, when the holder has several instruments from the same institution, the total amount loaded per month cannot exceed 10,000,000 CFA francs (around €15,250). As an example, the weekly total permitted by a Gabonese bank is 25,000,000 CFA

francs (around €38,000). In addition, in West Africa, the maximum amount of e-money that can be made available to a non-identified customer is 200,000 CFA francs (around €305) within a single month;

6. require systematic and effective reporting not just to the BEAC but also to national monetary authorities and to customs and tax authorities (for business transactions located out of their respective jurisdictions) based on a timeframe and framework set out by the BEAC. This data must be able to be refined based on requests from authorities tasked with carrying out investigations;

7. set out sanctions for non-compliance with regulatory provisions;

   Regarding mobile money in particular, regulatory provisions could help to minimise the identified risks by putting in place the following measures:

8. for risks linked to customers: for transactions between individuals, develop mechanisms to improve identification of the senders and recipients of electronic transactions and implement caps on the number of accounts, transaction frequency, and transfer volumes and amounts that can be made within a certain period of time; monitor the transaction flow system in order to alert the mobile money provider of any suspicious series of transactions (similar to the AML/CTF systems used by banks and fraud detection systems used by mobile telephone operators). The caps imposed would require criminals and terrorists to split their transactions, making them more likely to be detected by the system;

9. for risks linked to retailers: set out detailed verification procedures at the beginning of and throughout the relationship to reduce the risk to a low level;

10. for risks linked to agents, intermediaries and retail partners: implement detailed verification procedures at the beginning of and throughout the relationship as well as continuous monitoring of compliance with requirements.

5.2. Managing cybercriminal fraud risks

The attacks on a bank in the sub-region described above, as well as the cybercriminal typology, should lead the electronic money market regulator and the various stakeholders in the sector to ensure a robust security infrastructure is implemented, anticipating system changes that would allow detection of fraud and attacks as soon as possible or, in the worst case, facilitate prompt reactions to them.

5.3 Ensuring implementation of FATF Recommendation 15

Before launching new products or new business practices, or before using new or developing technologies, financial institutions, particularly sub-regional and national monitoring and regulatory bodies, each in their sphere, should take appropriate measures to manage and mitigate risks that may arise from (a) developing new products and business practices, including new delivery mechanisms, and (b) using new or developing technologies linked to new products or pre-existing products. Especially those linked to moves by mobile telephone operators towards issuing electronic money through VISA-type payment cards.

5.4. Coordinating the activities of stakeholders involved in managing NPMs

Regardless of the improvements that can be made to the legal framework governing new payment methods, they will have no effect if there are no instruments to ensure they are properly implemented. To do this, the possibilities presented by new IT solutions can be extremely helpful.

New technology could be used to implement a system that would improve coordination of and provide rigorous checks on the activities of stakeholders involved in NPMs for the purposes of preventing money laundering and countering terrorism financing by giving stakeholders a systematic overview of financial transactions carried out in the CEMAC using NPMs. At the same time, it would also centralise information (the volume and destination of funds, etc.) and allow rapid detection of money laundering and terrorism financing transactions using NPMs so that credit institutions, relevant criminal prosecution authorities and NAFIs could access and share information on declared payment incidents.

Such an IT- and telematics-based system would need to be connected to servers, to ATMs, to EPTs and to electronic payment systems managed by all stakeholders that issue e-money in the sub-region.

As an example, introducing transaction and account limits may be ineffective if, in terms of the way e-money is rolled out, there is a lack of interoperability between issuers' platforms in the sub-region— platforms fitted with blocking systems that are triggered whenever an attempt is made to exceed these caps. A technical solution could be put in place to instantly share information through a unique identifier assigned to each customer, managed by a central log of e-money holders. All of these measures should be given particular focus by the Groupement Interbancaire Monétique de l'Afrique Centrale (GIMAC—the Central African Electronic Money Interbank Group) as part of the development of its products but also as part of its statutory duties.

For the purposes of efforts to prevent money laundering and terrorism financing, this approach would facilitate the tracking of suspicious users within the CEMAC. It could highlight points at which NPMs are used, thus revealing routes along which e-money flows and via which financial criminals operate. By including fraud modules and programs to detect suspicious transactions (smurfing, etc.), this system could help to issue declarations of suspected money laundering and terrorism financing much more rapidly than individuals could. A fraudulent transaction involving several banks, considered by each bank to be nothing out of the ordinary, could nonetheless be detected from an overall viewpoint by this system.

However, for it to operate effectively, the recommendations given above would have to be implemented. It would also require the support and involvement of the stakeholders that are involved in offering NPMs, and, above all, support from political decision-makers. Less of a distant utopia than it might be imagined, establishing such a system is conceivable, and would contribute significantly to efforts to gain control over flows of money linked to NPMs and to reduce the risks of money laundering and terrorism financing that are linked to their use.

5.5 Building operational stakeholders' capacities

Effective application of anti-money laundering and counter-terrorism financing measures requires not only proper management of the relevant legislation in order to better understand the issue but also management of the risks of destabilisation that the misuse of payment instruments, including NPMs, can cause to financial sectors and economies as well as the damage it can do to national security.

Continuous high-quality training must therefore be provided to stakeholders working with NPMs. This training must cover knowledge of the legal framework of anti-money laundering and counter-terrorism financing measures and techniques for quickly detecting unusual transactions linked to new payment methods.

As such, the COBAC must work with the GABAC and/or financial intelligence units to issue guidelines (instructions) indicating the diligence measures specific to NPMs that e-money stakeholders should take to prevent the risks of money laundering and terrorism financing, as is the case with the French Prudential Supervision and Resolution Authority (ACPR). These guidelines should supplement the Regulation on the prevention and suppression of money laundering and of the financing of terrorism and proliferation in Central Africa of April 2016 and provide additional resources to build the capacity of all stakeholders in the NPM chain.

CONCLUSION

In accordance with its terms of reference, the objective of this typologies exercise was to report on developments in NPMs in the sub-region and to produce a comparative analysis of a range of regulatory approaches that could be used to regulate and monitor the phenomenon of NPMs and that maintain a balance between the need to promote, on the one hand, the inclusion of population segments that do not have access to the financial system and, on the other, the fight against money laundering and terrorism financing. It also aims to identify the specific risks and vulnerabilities inherent to pre-paid cards, online payment systems (including virtual money) and mobile telephone payment services. Finally, based on case studies located where possible in the sub-region, this report aimed to draw up procedures and to identify trends in the misuse of NPMs for money laundering and terrorism financing purposes in Central Africa.

Based on the data collected, particularly regarding the financial flows that result, this study reveals that the volume of transactions made using NPMs as defined above is increasing rapidly in the CEMAC, demonstrating that the segment of the population who would otherwise have no banking access has taken up the range of financial services offered to them through new payment methods, particularly mobile money.

However, these new methods of payment may present a number of inherent vulnerabilities to money laundering and terrorism financing.

These vulnerabilities are due to the following aspects:

- Shared by all NPMs considered in this report are regulatory shorcomings, the variety of stakeholders and the speed of technological developments;
- Pre-paid cards are vulnerable due to banks' lack of transparency, cardholder anonymity, non-compliance with the caps set by the BEAC, laundering of the proceeds of tax and customs fraud, circumvention of automatic declaration thresholds, and the way transactions are carried out.
- Mobile money is vulnerable due to customer behaviour, customer identification, retailers, agents, intermediaries and retail partners, and cross-border payments.

Two known cases of money laundering and terrorism financing linked to the use of NPMs in the CEMAC have been identified: the first case involved

computer fraud relating to pre-paid cards, resulting in money laundering, and the second involved money laundering via mobile money.

These different typological cases are, as discussed above, the result of the combination of several risk factors for money laundering and terrorism financing. These risk factors include those linked to weaknesses in the regulatory system. The main weakness is in the legal framework governing NPMs and its treatment of money laundering and terrorism financing aspects, an absence of texts governing the origin of funds, the identity of users, etc. Issues also arise from the way in which NPM activities are monitored and from transaction caps that are considered to be too high. Risk factors have also been identified regarding the supply of new payment methods and the way transactions are carried out.

To mitigate these risk factors and contain the risks of money laundering and terrorism financing, a number of recommendations have been made. These recommendations involve strengthening the regulations governing NPMs, proposing mechanisms to improve coordination between stakeholders involved in NPMs, and developing a system to collect real-time information on NPM transactions. Implementing this array of propositions through political will and concerted effort from all financial system stakeholders could make a key contribution to better management of NPM transactions and prevent the risks of money laundering and terrorism financing that are linked to the use of NPMs ■

APPENDIX 1

List of acronyms used in this report

AML/CTF: Anti-money laundering and counter-terrorism financing

BEAC: Bank of Central African States

BICEC: Banque Internationale du Cameroun pour l'Epargne et le Crédit

CEMAC: Central African Economic and Monetary Community

COBAC: Central African Banking Commission

EMI: E-money institution

GABAC: Groupe d'Action contre le Blanchiment d'argent en Afrique Centrale—Task Force on Money Laundering in Central Africa

GIMAC: Groupe Interbancaire Monétique de l'Afrique Centrale—Central African Electronic Money Interbank Group

ML: Money laundering

NAFI: National Agency for Financial Investigations

NPMs: New payment methods

TF: terrorism financing

UEMOA : West African Economic and Monetary Union

UMAC: Central African Monetary Union

APPENDIX 2

Bibliography

1 Adrianaivo, M, Kpodar, K, 2012, Mobile phones, financial inclusion and growth, Review of Economics and Institutions, Vol 3, No2 ;

2 Armendariz de Aghion, B., Morduch, J., 2005, "The economics of microfinance", The Mit Press Cambridge, Massachusetts London.

3 L'argent mobile au service des personnes non bancarisées (Maria Solin, Andrew Zerzan)

4 Attali, J., 2006, "La microfinance aujourd'hui", Planetfinance , télécharger à www.pointsdactu.org/article_print.php3?id_article=664.

5 Babajide, A, 2015, Financial inclusion and economic growth in Nigeria, International Journal of Economics and Financial Issues, Vol 5, No3,

6 CENAFE, 2010, Typologies et tendances en matière de blanchiment d'argent et de financement du terrorisme au sein des entreprises de services monétaires canadiennes - Rapport de typologies et de tendances de CENAFE.

7 CGAP, 2001, Commercialisation et dérive de la mission des IMF, la transformation de la microfinance en Amérique Latine, Etude Spéciale.

8 Chatain, P-L ., Hernandez-Coss, R., Borowik, K., Zerzan., 2008, Integrity in mobile phone financial services : Measures for mitigating risks from money laundering and terrorist financing, World Bank Working - Paper No 146.

9 Demetis, D., 2010, Technology and anti-money laundering : A systems theory and risks-based approach, Edgard Egar Publising Limited.

10 Di Castri, S, Mobile money: Enabling regulatory solutions, www.gsma.com/.../2013/.../MMU-Enabling-Regulato..

11 Donovan, K, 2012, Mobile money for financial inclusion, siteresources.worldbank.org/.../IC4D-2012-Chapter-4.

12 Helms, B., 2006, "La finance pour tous: construire des systèmes financiers inclusifs", Les éditions Saint-Martin.

13 Hulme, D., Mosley, P., 1996, "Finance against poverty", Volume 1, Routledge, London.

14 Investir au Cameroun, 2005, le Mobile money prend ses marques au Cameroun, N°38

15 Klein, M, Mayer, C, 2011, Mobile money and financial inclusion: The regulatory lessons, Policy research working paper 5664, World Bank.

16 Lal, R, Sachdev, I, 2015, Mobile money services, design and development for financial inclusion, Harvard Business School, Working paper 15-83

17 Lawack, V, 2013, Mobile money, financial inclusion and financial integrity: The South African Case, Washington Journal of Law, Technology and Art, Vol 8, No 3, p 317-346.

18 Lelart, M., 2002, L'évolution de la finance informelle et ses conséquences sur l'évolution des systèmes financiers, Réseau Entrepreneuriat, Cotonou 16-18 Avril.

19 Lelart, M., 2005, "De la finance informelle à la microfinance", Editions des Archives Contemporaines, AUF.

20 Levine, R, 2003, More on finance and growth: More finance, more growth ?, Federal Reserve Bank of St Louis Review, Vol 84, No 4, P31-46.

21 Mayoukou, C, 2000, La microfinance en Afrique centrale : Etat des lieux et perspectives de développement, TFD, 59-60, Juillet

22 Etude de TRACFIN, monnaie électronique, monnaies virtuelles et nouveaux risques.

23 Maria solin, Andrew Zerzan, L'argent mobile au service des personnes non bancarisées-2009

APPENDIX 3

List of regulatory texts regarding e-money

1 Regulation 01/02/CEMAC/UMAC/COBAC of 13 April 2002 on the conditions for the practice and management of microfinance activities in CEMAC countries.

2 Regulation 01/03/CEMAC/UMAC of 04 April 2003 on the prevention and suppression of money laundering and terrorism financing in Central Africa.

3 Regulation 02/03/CEMAC/UMAC/CM of 04 April 2003 on payment systems, methods and incidents.

4 Regulation 01/11/CEMAC/UMAC/CM of 18 September 2011 on the conditions for exercising the activity of issuing e-money.

5 COBAC regulation R-2005/01 of 1 April 2005 on diligence by establishments liable on matters of combating money laundering and of the financing of terrorism in Central Africa.

6 COBAC regulation R-2005/02 on e-money institutions.

7 COBAC instruction I-2006/01 of 31 July 2006 on information on the anti-money laundering and counter-terrorism financing system.

8 Instruction 01/GR of 31 October 2011 from the Governor of the BEAC on the monitoring of e-money payment systems, with an appendix including a reference framework featuring aspects to allow the BEAC to continue its work of monitoring activity

9 Instruction 02/GR/UMAC of 07 May 2014 from the Governor of the BEAC on the implementation of multibanking as part of the issuance of e-money


GROUPE D'ACTION CONTRE LE BLANCHIMENT D'ARGENT
EN AFRIQUE CENTRALE
G.A.B.A.C

Immeuble de la BVM AC - place de l'Indépendance
P.O. Box: 764 Libreville - Gabon - Tel.: +241 01 76 39 54
E-mail: secretariat@spgabac.org - www.spgabac.org