Association des Banques Centrales Africaines

Association of African Central Banks

CONTINENTAL SEMINAR OF THE ASSOCIATION OF THE AFRICAN CENTRAL BANKS ON THE THEME 'FINANCIAL TECHNOLOGY INNOVATIONS, CYBERCRIME: CHALLENGES FOR CENTRAL BANKS'

N'Djamena, Chad, 14 - 16 May 2018

****** / ******

CONCLUSIONS AND RECOMMENDATIONS

---

1. INTRODUCTION

The 2018 AACB Continental Seminar was hosted by the Banque des Etats de l'Afrique Centrale (BEAC) and held on 14 - 16 May 2018 in N'Djamena, Chad, on the theme 'Financial Technology Innovations, Cybercrime: Challenges for Central Banks'. Fifty-three (53) delegates from twenty-one (21) member Central Banks, six (6) regional and international institutions and one (1) University attended the seminar. The list of participants is attached as appendix.

2. OPENING CEREMONY

The opening ceremony was chaired by Mr. Ivan Bacale Ebe Molina, Director General of Studies, Finance and International Relations of the BEAC.

In his introductory remarks, Mr. Papa Lamine Diop, Executive Secretary of the AACB, on behalf of the AACB Chairman, Mr. Lesetja Kganyago, Governor of the South African Reserve Bank (SARB), expressed deep gratitude to Honourable Abbas Mahamat Tolli, Governor of the BEAC, for hosting this important event of the Association and for the excellent arrangements made. He appreciated the generous hospitality of the Chadian people and expressed the warmest thanks to His Excellency, President Idriss Deby Itno, the Government and the people of Chad.

He thanked the experts for accepting to share their knowledge on the topics which were going to be discussed at the seminar as well as the representatives of regional and international institutions for their multifaceted support to the AACB. Moreover, the Executive Secretary commended the remarkable participation of AACB member central banks as a testimony of their strong determination to contribute in tackling the challenges which have potential to impact monetary integration in Africa.

He pointed out that the Continental Seminar is taking place in a context characterized by a sustainable development of innovations in information technologies which brings about the emergence of new actors, products and business models affecting the main functions of central banks and bring with them new cyber-risks.

In this regard, the Executive Secretary indicated that the seminar should primarily contribute to a better understanding of the opportunities offered by Fintech, with a view to facilitating financial transactions and accelerating financial inclusion. It should also aim at providing a relevant analysis of the challenges and risks of Fintech and reflect on strategies for harnessing the benefits of Fintech while avoiding inherent risks which could promote fraud, money laundering and the financing of terrorism that could jeopardize the stability of financial systems in Africa.

In his opening speech, the Director General welcomed the delegates and wished them a pleasant stay in N'Djamena. He also conveyed the apologies of the Governor of the BEAC, Mr. Abbas Mahamat Tolli, who would have liked to preside at the ceremony but could not be present due to other commitments.

Mr. Bacale Ebe Molina noted that a large number of central banks represented was a reflection of their keen interest in AACB activities, particularly those aimed at addressing the challenges of African monetary and financial integration. He added that the theme was timely, especially in view of the rapid development in Fintech and their impact on the economies of Member States. Moreover, the sharing of practical experiences between respective institutions was enrichment that would lead to fruitful outcomes.

The Director General mentioned some work already engaged within the BEAC to which the conclusions of the Seminar could make a contribution. These actions included the methods of supervision to be adopted in order to reduce risks associated with the emergence of financial innovations which could impact financial stability. They also covered the practice of de-risking and the appropriate measures that can mitigate its impact on the banking sector.

He added that the BEAC, in consultation with the Banking Commission of Central Africa, has developed specific community texts which regulate the conditions for approval, execution and control of the activity of electronic money issuing institutions. Other regulations in force on the security of the information systems of credit and microfinance institutions set obligations on these institutions with regard to the quality of accounting and financial information, the integrity and confidentiality of transactions, the preservation and availability of information, computer system security as well as computer backup systems.

He noted that more recently, the BEAC took a decision to establish ceilings for transactions via electronic payment instruments in order to ensure the adequate liquidity of the institutions issuing electronic money and to prevent money laundering and financing of terrorism.

In conclusion, the Director General wished the delegates constructive deliberations and hoped that the Continental Seminar would meet its objectives. In declaring the seminar open, he invited participants to carefully note the key lessons from the seminar that should contribute to the promotion of monetary and financial stability in Africa in the coming years and decades.

3. STRUCTURE OF THE SEMINAR

The Seminar was structured as follows. Three sub-themes were presented by resource persons. Representatives of central banks then shared their experiences. Finally, three break-out sessions were organized to discuss specific topics and to reflect on the actions to be taken by the central banks in order to benefit from the innovations in Fintech and to make recommendations to be presented to the Assembly of Governors for consideration.

3.1. Plenary Session 1: Presentation of the Sub-themes

The following three sub-themes were presented respectively by Dr. Sean Maliehe, Post doctoral Fellow, Human Economy Programme, Center for Advancement of Scholarship, at the University of Pretoria, Mr. Adrien Delcroix, Market infrastructure expert, Directorate General Market Infrastructure & Payment – Oversight Division at European Central Bank (ECB) and Mr. Danny Brando, Vice President, Supervision Group Cybersecurity Policy, at the Federal Reserve Bank of New York (FRBNY):

- The Digital World and a Human Economy: Mobile Money, and Socio-Economic Development in Africa;
- Fintech: Opportunities and Challenges for African Central Banks;
- Cybersecurity: Implications for Supervisory Practices.

Mr. Delcroix and Mr. Brando made their presentations by videoconferencing, from the ECB in Frankfurt and the FRBNY in New York respectively.

In his presentation, Dr. Maliehe pointed out that the use of a microcomputer, internet connectivity or the availability of electricity is still a privilege of a few in Africa. The Internet access rate is 35.2% on average on the continent, below the world average of 54.4%. However, mobile phone penetration has recorded higher statistics. In 2011, there were 445.6 million mobile phone users in the Middle East and Africa. In both regions, the

statistics reached 745.1 million in 2018. He indicated that the mobile phones were no longer a sign of wealth, prestige and privilege. They have become a key factor of financial inclusion for a large part of the African population and are indispensable and flexible forms of technologies in daily communication and the organization of economic activity.

Dr. Maliehe mentioned the success of mobile money in several African countries, including Kenya, Lesotho and Zimbabwe, where innovative services have fundamentally changed the way in which people expand their social networks. Mobile money has made it easier to access transparent digital transactions and better manage their financial activities. It has also been a gateway to other financial services, such as insurance, savings and credit. Moreover, mobile money has led to increased economic growth by providing to businesses the means to grow by training a generation of emerging market managers.

In light of these developments, the presenter argued that mobile money and related innovations can be considered as socio-economic gains for people in Africa and elsewhere. These advantages justify the consideration that development experts and governments are making efforts to encourage the use of innovations to facilitate the financial inclusion of populations in the South.

He further argued that mobile money is built around a set of actors with competing interests and generally the interests of the companies outweigh those of the people. Consequently, the implementation of innovations should not depend only on technical, legal and regulatory factors but also on the understanding of the socio-economic conditions of populations.

In the light of these observations, Dr. Maliehe indicated that it is necessary to broaden the role of central banks and other regulators to effectively manage businesses and protect the interests of the population. He urged central banks to realize that digital finance is not a global panacea. Some situations require that prior studies be conducted so that poor people can derive socio-economic benefits from mobile money and digital payments.

The second sub-theme on '*Fintech: Opportunities and Challenges for African Central Banks*' was presented by Mr. Adrien Delcroix of the European Central Bank. He first defined Fintech as technologically enabled financial innovation that could result in new business models, applications, processes or products with associated material effect on financial markets and institutions and the provision of financial services.

His communication mainly centered around the key Fintechs products and services, the drivers of Fintech innovations, the implications for the structure of the financial sector and the risks and opportunities of Fintechs as well as the role for central banks and regulators.

In terms of the key Fintech products and services, he identified three sectoral innovations: (1) credit, deposit, and capital-raising services (e.g. crowdfunding, mobile banks and credit scoring, etc.), (2) payments, clearing and settlement services which could be in retail (e.g. mobile wallets, peer-to-peer transfers and digital currencies) or in wholesale (e.g. value transfer network, foreign exchange (FX) wholesale and digital exchange platform) and (3) investment management services (e.g. high-frequency trading, copy trading, E- trading and robot-advice). Beside these key products and services, he mentioned the market support services, including portal and data aggregators, distributed ledger technology (blockchain, smart contracts), internet of things/mobile technology and artificial intelligence, ecosystems, security and cloud computing.

Mr. Delcroix added that shifting of customer expectations and evolving technology, and in particular the internet, big data, mobile technology and computing power, are the main interdependent drivers of Fintech innovations, as well as changes in financial regulation and market structure. He argued that the impact of Fintech innovations on the banking industry will depend on the adoption rate of the underlying technology in society and the degree and pervasiveness of technological know-how within the general population. He noted that the faster the pace of change, the more is its impact on society.

With respect to the implications for the structure of the financial sector, Mr. Delcroix indicated that three broad scenarios could be envisaged: banks might embrace the digital trend and team up with Fintechs; Fintechs might break up the value chain of banking and banks would end up losing revenue, market share and direct contact with clients; Fintechs could be swallowed up by big tech, such as Ali Baba or other retail chain.

Mr. Delcroix identified the risks of Fintechs innovations on consumer sector and on banks and the banking system. With respect to the risks on consumer sector, he mentioned data privacy, data security and discontinuity of banking services in particular. On the risks on banks and the banking system, he noted especially risks that are of a strategic nature and those that affect profitability as well as those relating to cyber-risk, money laundering and risks associated with the financing of terrorism, as well as the liquidity risk and risks related to the changing sources of bank funding.

However, he added that Fintech innovations offer opportunities for consumers, as well as banks and the banking system. For consumers, this includes financial inclusion, the provision of better and more tailored and faster banking services and the lower transaction costs. For banks and the banking system, he noted improved and more efficient banking processes, the innovative use of data for marketing and risk management purposes, the potential positive impact on financial stability due to increased competition and RegTech.

Presenting the role for central banks and regulators, Mr. Delcroix indicated that innovations in the financial sector impact the way authorities conduct regulatory activities and regulatory initiatives also affect the direction and speed of transformation in the financial sector. He recommended that to create an innovation-friendly environment, central banks and regulators need to carefully balance the benefits for companies and households with the potential risks. They also need to review the regulatory framework in order to ensure that it is technology neutral and maintain a level playing field between new entrants and incumbents while taking into account different levels of risks. In order to promote efficient and secure payment services, they should avoid fragmentation by promoting technical standardisation and interoperability and enhance cyber-resilience by encouraging market participants to invest in a fully-fledged cybersecurity strategies and response plans.

The third sub-theme on '*Cybersecurity: Implications for Supervisory Practices*' was presented by Mr. Danny Brando of the Federal Reserve Bank of New York. The presentation focused on the Federal Reserve System supervision, the positive observations beyond IT hygiene and the supervisory approach.

Introducing his presentation, Mr. Brando indicated that the Federal Reserve supervision mission is to promote the stability of the financial system and seeks to minimize and contain systemic risks through active monitoring and engagement in the United States (US) and abroad. The Federal Reserve System supervision is also aimed at promoting the safety and soundness of individual financial institutions and monitoring their impact on the financial system as a whole.

Empirically, Mr. Brando reported troubling statistics. The Ponemon Institute 2017 cost of a data breach study revealed that the average time to identify a breach is 191 days. Moreover, according to the 2017 Verizon Data Breach Report, a proportion of 24% of all cyber breaches and incidents affected financial institutions – the highest of all sectors – and 73% of cyber breaches were financially motivated.

In addition, these breaches have allowed the Federal Reserve System to make several positive observations beyond IT hygiene. They made it easier to identify and understand the threats, with the view to provide an adequate response. To this end, there should be a simplification of the infrastructure and standardized security control practices. Positive observations have also been made and related to integration into enterprise risk management and understanding at the Board of Director level. Moreover, emphasis should be placed on developing and retaining cyber talent. There should also be relevant

infrastructure that is resilient enough to cybercrime. Thus, the goal is to empower industries, so as to give them the means to prevent all kinds of attacks.

With regard to the supervisory approach, he explained that all US institutions rely primarily on the National Institute of Standards and Technology (NIST) voluntary framework and the Federal Financial Institution Examination Council (FFIEC) information technology handbook. The supervisory approach is also based on US financial regulators harmonizing their approaches to cybersecurity supervision. The approach adopted also involves participating in domestic and international efforts to identify and address cyber risks to the financial sector. It aims at leveraging data to analyze the business and technology interconnectedness of critical financial markets. The Federal Reserve System requires firms to continuously improve basic IT hygiene.

In conclusion, Mr. Brando said that to ensure survival from cybersecurity, it is necessary to focus on education and to have multiple passwords.

3.2. Plenary session 2: Experiences of AACB central banks

Ten AACB member central banks presented their experiences in relation to the central theme of the Seminar.

4. BREAK-OUT SESSIONS

Delegates deliberated on three topics in the break-out sessions.

Break-out session I: 'Implications of Fintech (including digital currencies and blockchain technologies) on monetary policy and financial stability in Africa'

Observations

1. The areas of Fintech innovation identified for discussion were: mobile money; cryptocurrencies and distributed ledger technology (DLT); artificial intelligence (AI), including the use of machine learning (ML) supported by the growth in big data; and biometrics.
2. It was noted that mobile money has footprints in most countries, but has not been successful in some countries. Mobile money was initially used as a means of money transfer. It now offers credit, savings and insurance services.
3. Mobile money promotes financial inclusion by bringing more people into the formal financial system which enhances the monetary policy transmission mechanism.
4. Cryptocurrencies were deemed to have the biggest potential impact on monetary and financial stability despite their current limited use.
5. A distinction was noted between the concepts of private cryptocurrencies, such as bitcoin, Ethereum and Monero versus central bank digital currencies (CBDC).
6. There are different views on the approach to cryptocurrencies ranging from potentially starting to regulate exchanges to banning the acceptance of cryptocurrencies by banks.
7. AI analytics could be used to perform financial stability assessments, regulatory oversight, open market operations, credit assessment, investment advice, etc. Biometrics

could also be used for identification and authentication in providing safer financial services.

8. Regulatory arbitrage. Due to the cross cutting nature of the services for mobile money, regulation involves mobile network operators and financial services regulators.
9. There are currently no agreements on how cryptocurrencies should be defined and their regulatory treatment is therefore uncertain. Globally some consider them as currencies while others view them as commodities.

Recommendations

1. Service providers should promote interoperability between services.
2. Central banks should develop or update regulatory frameworks to embrace current Fintech innovations.
3. Central banks should collaborate on information sharing on Fintech developments, cyber and illicit activities.
4. Central banks should play a financial literacy role in making sure that citizens understand new technologies.
5. Central banks should continue to monitor Fintech developments with a view to ensuring timely development of regulatory frameworks, such as the definition of cryptocurrencies. In this regard, central banks should consider setting up structures such as Fintech units and regulatory sandboxes.
6. **The AACB should set up a Fintech taskforce team to align approaches on Fintech developments.**

Break-out session II: Mobile Financial Services (MFS): Overview - Potential Risks and Challenges as well as Recommendations for African Central Banks

Introduction

Innovations in Fintech have brought in opportunities for the private sector and the Central Governments and Banks to offer financial services to the previously unserved and underserved communities in Africa. The mobile devices, in particular, have moved from being luxuries or status symbols to become necessities. The devices have been used as access channels to the financial services.

Financial services that can be provided through mobile devices include:

1. Payment and Remittances
2. Bank Credit and Savings
3. Insurance and Assurance Services

4. Security and Investment Management
5. Market Support

Potential Risks/Challenges

1. **Non-compliance with anti-money laundering (AML) / combatting the financing of terrorism (CFT) legislation**

   In some jurisdictions in Africa, official identity documents and SIM card registration are not in place for identification which can be a challenge to AML/CFT compliance.

2. **Cybersecurity risks**

   Mobile financial services are prone to cybersecurity threats due to various players in the value chain such as banks, telecoms, solution providers and end users – consumers of the mobile services.

3. **Regulatory arbitrage**

   There are various parties involved in the provision of mobile financial services which fall under the ambit of different regulators. Different standards and regulations may lead to conflicting and divergent perspectives which creates the opportunity for regulatory arbitrage.

4. **Unclear responsibility for consumer and data protection**

   The involvement of various stakeholders in the provision of the mobile financial services may lead to confusion as to who is responsible for the protection of the consumer.

5. **Service provider resilience issues**

   In some jurisdictions service providers are not able to ensure the continuous availability and timely recovery of services. This affects quality of service and deters consumers from using mobile financial services.

6. **Taxes, high interest rates and charges**

   Taxes imposed by governments on mobile payment transactions make them costly to the customers, which is in contradiction to financial inclusion agenda. Furthermore, high rate of interest and charges on the services are a major bottleneck to the development of the mobile financial services.

Recommendations

1. **Local and regional collaboration among regulators (MoUs) and key stakeholders**

   There is a need for different regulators involved in the provision of mobile financial services to collaborate.

2. **Risk based - regulation and supervision**

   A risk-based and proportionate approach must be adopted instead of traditional and standards based approach to supervision. Regulators should embrace technology to the supervision framework.

3. **Legal, AML/CFT & cybersecurity frameworks**

   Frameworks for legal, AML/CFT and cybersecurity should be in place.

4. **Guidelines and regulations**

   Guidelines and regulations issued for the provision of mobile financial services should be periodically reviewed and assessed to take into account innovations.

5. **Credit reference bureaus compulsory**

   All mobile financial services providers should be interfaced with the credit reference bureau so that proper credit worthiness of the customer and providers are verified in real time. The central bank should ensure that the credit reference bureau are in place and fully functional.

6. **Consumer education**

   Regulators should ensure that service providers and regulators have a consumer education program in place to avoid wrong and malicious uses of these services.

7. **Consumer friendly interface**

   The service providers should ensure that interfaces for mobile financial services are designed in such a way that it addresses the needs of different consumer segments.

8. **National strategies are key for the success of the mobile financial services**

   National strategies for the promotion of mobile financial services should be developed.

Break-out session III: Cyber security and financial stability: Challenges for African Central Banks

Observations

There are many examples of large scale cyber incidents to illustrate the importance of cyber security for safeguarding financial stability.

A number of cyber risk areas that are driving the prominence of cyber security within the context of central banks and the international financial system include:

1. Financial fraud – In broad terms, this can be separated into two areas:

   a. Retail – Cyber fraud targeting payment systems including internet banking, mobile money payments and the like.

   b. Wholesale and Reserves/Central Bank holdings – Larger financial fraud like the Swift related fraud we have seen on central bank reserves and the potential impact to wholesale payment systems.

2. Espionage – Sensitive data/information leakage

   a. Leakage of sensitive information supporting or about central bank policy decisions could have far reaching impact for central banks.

   b. Leakage of other sensitive information like board reports could expose central banks.

3. Disruption of critical infrastructure

   a. Due to the critical role central banks play and the provision of RTGS systems it could be a key target.

   b. Regionally focussed attacks are also possible.

   c. What needs to be considered is not only the central bank infrastructure but also the underlying infrastructure for example electricity and service providers.

4. Reputational damage affecting trust may result from a cyber breach.

Challenges

Interconnectivity and interconnectedness of the financial players including central banks create the context within which these challenges need to be addressed. These include:

1. Inadequate skills, resource and capacity – There is a lot of deep cyber skills across African central banks but demand is far outstripping supply.
2. Cyber security awareness/digital literacy – Banks are vulnerable to cyber threats due to behavioural issues, specifically as a result of an ever changing threat landscape.
3. The lack of standardised policies, guidelines and laws makes African central banks vulnerable due to inconsistent security measures being applied.
4. Software security updates and complexity and skills around management of software makes central banks vulnerable to attacks.
5. Lack of adequate asset management is a big vulnerability as it is difficult to protect infrastructure and information if you are not aware of the landscape.
6. Lack of segregation of duties due to the size of institutions is a specific vulnerability within the African context.
7. There is inconsistent focus on cyber resilience and testing of recovery arrangements.
8. There is no standardised penetration testing and assessment that is widely accepted to ensure cyber readiness.
9. There is a challenge in establishing a mature detection/monitoring and response capability.
10. Lack of information sharing and intelligence within the various institutions across the AACB.

11. Malicious insiders exploiting vulnerabilities remain one of the major concerns.
12. There has been an increase in compromises through third party service providers.
13. The physical security threats impact cyber security directly.

Recommendations:

1. Each central bank should design and implement a cyber security programme that addresses the various aspects around setting up an internal capability that ensures the prevention, detection and response to cyber incidents. The programme must be aligned to international best practice and should enable collaboration.
2. Establishment of a cross-departmental cyber security group (involving all key stakeholders and affected departments) within each central bank. This working group needs the appropriate level of board and senior management support, covering all the major areas recommended by international best practices and regulations (e.g. CPMI-IOSCO, BIS CPMI Wholesale Payment Security Task Force, ISO, NIST, SWIFT CSP).
3. Collaboration across central banks should share internal information and skills. Collaboration should also include underlying financial institutions as soon as this is feasible as underlying structures within each jurisdiction is required to facilitate this. This will necessitate the expansion into collaboration on national, regional and international level. This should include governments and other key national stakeholders.
4. **The AACB should facilitate the establishment of a cyber working group / task team covering the following areas**:
    a. Oversight, prevention and regulation:
        i. Sharing information about laws, regulations, frameworks and practices to have a consistent approach across Africa.
        ii. Evaluating the potential to assess cyber readiness across central banks based on a common measurement approach.
        iii. Explore standardised assessments of cyber threats (e.g. CBEST, TIBER-EU)
    b. Cyber threat and intelligence sharing:
        i. Sharing of threat information that has a bearing across central banks that can assist in detection.
        ii. Define information sharing protocols (e.g. using traffic light systems indicating who it can be shared with).
        iii. Setting up sharing platforms and technologies (e.g. MISPs) to enable real time effective sharing of underlying technical threat information.
    c. Cyber response and recovery:
        i. Setting up communication structures to coordinate cyber response to incidents reaching across the continent and internationally.

ii. Holding cyber simulations to test cyber readiness across AACB members.

d. Cyber skills development programmes for member central banks, including:

i. Secondment of resources through partnership programmes.

ii. Training seminars and onsite visits facilitated by the AACB for skills transfer and peer learning.

iii. Forming international partnerships to assist in skills development with other central banks and financial sector role players.

5. CLOSING CEREMONY

The closing ceremony was chaired by Mr. Annour Mahamat Hassan, the National Director of BEAC for Tchad. It was marked by the presentation of the conclusions and recommendations of the seminar. Thereafter, the participants expressed gratitude to His Excellency President Idriss Deby Itno, to the Government and the people of Chad, as well as to the Honourable Governor Abbas Mahamat Tolli and the staff of the BEAC for their warm hospitality. In declaring the seminar closed, Mr. Hassan noted that the conclusions of the seminar would provide critical inputs towards ensuring financial stability, more financial inclusion and better monetary policy implementation in Member Central Banks and wished participants safe trips back to their respective destinations.

Done in N' Djamena, Chad, 16 May 2018

Appendix

LIST OF PARTICIPANTS

NOM/NAME	TITRE/TITLE	INSTITUTION	Email
1.M. Josephate Zola	Adjoint / Directeur	**BCEAO**	jzola@bceao.int
2.M. Mohamed Traoré	Chef de Service		motraore@bceao.int
3.M. Annour Mahamat Hassan	Directeur National	**BEAC**	annour@beac.int
4.M. Taoukreo Hemwue	Adjoint / Directeur National		taoukreo@beac.int
5.M. Abba Fanta Madji	Adjoint / Directeur National		abbe@beac.int
6.M. Eloundou Ndeme Jacques	Chef de service		jeloundou@beac.int
7.M. Ducor Mshaa	Chef de service		ducor@beac.int
8.M. Mbede Jean-luc	Responsable Sécurité		mbedejl@beac.int
9.M. Siazo Gini Frederic	Directeur	**BANQUE CENTRALE DU CONGO**	siazo@bcc.cd
10.M. Tshilumba Wa Tshilumba	Manager		tshilumba2050@gmail.com
11.Mr. Ahmed Monir Mohamed	Fintech Specialist	**CENTRAL BANK OF EGYPT**	ahmed.monir@cbe.org.eg
12.Mr. Sheriff Touray	Principal Economist	**CENTRAL BANK OF THE GAMBIA**	shtouray@cbg.gm
13.Dr. Settor Kwabla Amediku	Director	**BANK OF GHANA**	settor.amediku@bog.gov.gh
14.Mr. Michael Ewusi Mensah	Director		michael.mensah@bog.gov.gh
15.Mr. Simon Gichuki	Manager Bank Sup.	**CENTRAL BANK OF KENYA**	gichukisg@centralbank.go.ke
16.Mr. Mike Ombuna	IS Auditor, Bank. Sup.		Ombunamg@centralbank.go.ke

17.Mr. Diakae Al Lewis	Assistant Director	**CENTRAL BANK OF LIBERIA**	dallewis@cbl.org.lr
18.José J. Randriamampionona	Respons. Cont. Séc.	**BANKY FOIBIEN'I MADAGASIKARA**	jj.randriamampionona@bfm.mg
19.M. Saadna Ahmed Jiddou	Directeur	**BANQUE CENTRALE DE MAURITANIE**	saadna@bcm.mr
20.M. Ahmed Baba Moussa Welad	Chef de projet		abwelad@bcm.mr
21.Mr. Gawtam Raiy Kallychurn	Chief Inf. Security Officer	**BANK OF MAURITIUS**	Gawtam.kallychurn@bom.mu
22.Mr. Aderito Abilio Pilica	IT Examiner	**BANK OF MOCAMBIQUE**	aderito.pilica@bancomoc.mz
23.Mr. José Nelson Da Costa Brazäo	Information Sec. Analyst		nelson.brazao@bancomoc.mz
24.Dr. Isa Audu	Deputy Director	**CENTRAL BANK OF NIGERIA**	iaudu@cbn.gov.ng
25.Mr. Victor Ugbem Oboh	Assistant Director		voboh@cbn.gov.ng
26.M. Nimersio Trindade	Directeur Adjoint	**BANCO CENTRAL DE SAO TOME E PRINCIPE**	ntrindade@bcstp.st
27.M. Djalma Trovoada	Tech. Informatique		dtrovoada@bcstp.st
28.Mr. Morlai Bangura	Director	**BANK OF SIERRA LEONE**	mbangura@bsl.gov.sl
29.Mr. Crispin D. George	Assistant Director		cgeorge@bsl.gov.sl
30.Mr. Francis Selialia	Senior Manager	**SOUTH AFRICAN RESERVE BANK**	francis.selialia@resbank.co.za
31.Mr. Gerhard Cronje	Head – Cyber & Info. Sec.		gerhard.cronje@resbank.co.za
32.Mr. Gerhard Van Deventer	Senior Fintech Analyst		gerhard.vandeventer@resbank.co.za
33.Mr. Jabulane Caiphas Dlamini	Head - Financial Sector Strategy	**CENTRAL BANK OF SWAZILAND**	jabulaned@centralbank.org.sz
34.Ms. Philile Nxumalo	General Manager		phililen@centralbank.org.sz
35.Mr. Bhekisisa Sicelo Tsabedze	Economist		bhekisisat@centralbank.org.sz
36.M. Enis Belhassen	Directeur	**BANQUE CENTRALE DE TUNISIE**	enis.belhassen@bct.gov.tn
37.M. Abderrahmen Miled	Sous-Chef de Service		abderrahmen.miled@bct.gov.org
38.Mr. Enoch Kasajja Matovu	Risk Quantitative Analyst	**BANK OF UGANDA**	ematovu@bou.or.ug
39.Ms Kugonza Rose Kuteesa	Head-Inf &Publication		rkuteesa@bou.or.ug
40.Mr. Mathews Lungu	Acting Director -ICT	**BANK OF ZAMBIA**	plungu@boz.zm

41.Mr. Nicholas Masiyandima	Principal Economist	**RESERVE BANK OF ZIMBABWE**	nmasiyandima@rbz.co.zw
42.Mr. Douglas Muranda	Head Oversight & Risk Manag.		dmuranda@rbz.co.zw
43.Dr Lucas Kamau Njoroge	Economist	**COMESA MONETARY INSTITUTE**	lnjoroge@comesa.int
44.Mr. Alieu Ceesay	Principal Economist	**AMAO / WAMA**	aoceesay70@yahoo.com
45.Mr. Ismaila Jarju	Director	**WEST AFRICAN MONETARY INSTITUTE**	ijarju@wami-imao.org
46.Dr. Morenakemang Sean Maliehe	Post - Doctoral Researcher	**UNIVERSITY OF PRETORIA**	seanmaliehe@gmail.com
47.Mr. Mark Yeon Wook Choi	Manager CBIAS	**FEDERAL RESERVE BANK OF NEW YORK**	mark.choi@ny.frb.org
48.M. Hugues Tsafack Kamewe	Financial Sector Advisor	**MAKING FINANCE WORK FOR AFRICA**	h.kamewe-tsafack@afdb.org
49.M. Jean Claude Nachega	Représentant Résident	**FOND MONETAIRE INTERNATIONAL**	jnachega@imf.org
50.Mr. Papa Lamine Diop	Executive Secretary	**AACB SECRETARIAT**	pdiop@bceao.int
51.Mr. Acho Theodore Yapo	Research Officer		atyapo@bceao.int
52.Mr. Balamine Diane	Research Officer		bdiane@bceao.int
53.Mr. Arthur Konan Koffi	Webmaster		kyakoffi@bceao.int