Regulating Internet Banking In Nigeria : Some Success Prescriptions– Part 2

Journal of Internet Banking and Commerce, April 2006, vol. 11, no.1 (http://www.arraydev.com/commerce/jibc/)

Abel Ebeh Ezeoha (Mr.), Department of Banking and Finance, Ebonyi State University, Abakaliki , Nigeria

Email: aezeoha@yahoo.co.uk

Ezeoha is a lecturer in the Department of Banking and Finance, Ebonyi State University , Abakaliki Nigeria . His special areas of research interest include development banking, marketing of financial services, innovations in banks' products and services, and cross-border financing. He is a financial consultant and investment analyst. He had before now worked as a research assistant under Professor Chibuike U. Uche, Department of Banking and Finance, University of Nigeria , where he is currently a PhD candidate. As a principal lecturer in “Marketing of Banking Services”, he had designed a course programme to reflect various areas of current developments in electronic banking, finance and commerce.

Abstract

This paper is the second part of an earlier one on the problems and challenges of Internet banking regulation in Nigeria . The paper argues that for Internet banking to assume a developmental dimension in Nigeria and for the country to be fully integrated in the global financial environment, the prevalent level of frauds in Nigeria (and among Nigerians) must first be addressed. It suggests that the ways to do this are first to: get the relevant local laws in place and in consonance with international laws and conventions; get the citizens well educated on the intricacies of Internet usage and frauds, as well as the regulatory implications of wrong/fraudulent uses of the Internet; ensure that all the major background problems such as poverty, corruption and bad governance are addressed and; ensure adequate interface and collaborations between Nigerian local law enforcement agents and the various international agencies that are presenting pursuing the course for safe Internet community.

Introduction

As the development and spread of Internet banking continues across countries, one of the most critical areas where the impact of the change is being felt is the structure and instrument of banking regulation. At the same time, calls for increased regulatory emphasis have equally been intensified. This has mainly arisen because, in the words of Norgren (2001), “the logic of Internet has already today shaped markets and financial institutions for a while, and it is now high time to draw relevant regulatory

conclusions from this development". Explaining this regulatory dynamic, Spong (2000) illustrated that "electronic banking, by speeding up transactions, creating new competitors and services, altering banking operations and support functions, and dramatically expanding the reach of financial institutions, is leading to many significant changes in our deposit and payments system; and have joined to raise several issues for banking regulation and its objectives of depositor protection, monetary stability, an efficient and competitive banking system, and consumer protection". Again, given the inherent nature of Internet banking in eliminating paper documentation and traditional identity verification processes, there are clear reasons to believe that new dimensional risks are created (Wright, 2002) and that new regulatory and supervisory challenges are thrown open to national and international governments.

Apart from the above changing dynamics brought by the growing reliance on Internet, other issues that have joined to increase regulatory concerns for Internet banking include the prevalence of frauds in the Internet environment. As is posited by Williams (2002), organized crimes have increased in line with the increased use of Internet. Hence in a country like Nigeria where cases of fraudulent uses of Internet are rampant, regulating Internet banking becomes not only a national concern, but also attracts some international attentions. At the same time, the capacity of the existing regulation to adequately address the complexities created by this mix-up remains very doubtful (Ezeoha, 2005a). In which case, using the conventional banking laws and policies to address cyber transactions is thus inconsistent. This has been mainly so because most of the existing national banking laws were designed and formulated before the advent of Internet (Wallsten, 2003). In effect, much of the current regulatory and supervisory apparatus governing the operations of banks were designed based on physical location, as against the remote (and sometimes virtual) system of Internet banking. Even at present, there are no enforceable cyber crime regulations in most of the developing African countries, Nigeria inclusive, and where such laws exist they are hard to enforce (Udotia, 2005). For some countries therefore, the elementary stages of Internet development evolved without any definite regulatory structure on ground.

Generally, regulating Internet banking encompasses three major issues: how bank customers are to be protected; how banks are to be protected; and how the country would be protected against the negative publicity associated with the spread of Internet frauds. Whereas bank customers may be concerned with being able to get Internet banking services at more convenient, speedy, safe and cost efficient way (Awamleh et al. 2003), the concern of banks generally is on how to get the best out of Internet banking in terms of cost efficiency, competitive advantage and enhanced profitability, especially in comparison with the opportunity cost of similar services and investments in conventional banking system. On the other hand, the focus of national government is to ensure that there is organized and structured developments in the entire electronic banking system in such a way that such development would contribute optimally to the stability of the financial system, and the development of the economy in general. Regarding the latter, regulatory appeals also cover the issue of protecting the national financial system against global leakages that may be caused by financial and economic crimes that are known to be perpetrated through the Internet.

In the case of Nigeria , effective regulation, especially of Internet banking operations have become very necessary. The country, which is an English-speaking nation, has high repute for Internet fraud the world over; it is highly populated and has the largest market in Africa; economic and political corruptions are rampant and persisting; poverty and unemployment among young men and women are almost as high the country's population; it has the fastest growing ICT market in Africa and; its banking system is currently facing the largest industry convergence in the history of banking in Africa. Locally, official ranking of ICT development in the country shows that Nigeria is in a prime position in Africa as No. 1 GSM country in West Africa and No 2 in Africa, No. 1 Fastest growing telecom market in the world, No. 1 in Telecom regulation in Africa ? No. 1 fixed wireless country in Africa, No. 1 for low international call tariff in Africa, No. 1 in lowest cost of Sim packs in Africa, No. 1 in enabling laws and regulations in Africa?, No. 1 Revenue per user, No. 1 Transparent spectrum auctioning in Africa, No. 1 in consumer education and empowerment in Africa and No. 1 Liberalized market in Africa (ThisDay December 28, 2005) . Most of the claims are however questionable at least in part, given the growing reputation of Nigeria as a safe heaven for ICT frausters.

With these mixed developments, it is clear that the country needs adequate regulatory cover to face the global Internet development train. Expectedly, emphasis to this effect should be to first update the existing national regulations on banking and finance in line with international standards; develop structures and agencies capable of enforcing these laws; get the citizens well educated on the intricacies of Internet usage and frauds, as well as the regulatory implications of wrong/fraudulent uses

of the Internet; ensure that all the major background problems such as poverty, corruption and bad governance are fully addressed and; ensure adequate interface and collaborations between our local law enforcement agents and the various international agencies that are presently pursuing the course for safe Internet cyber community.

The rest of the paper reviews the existing local and global efforts towards safeguarding the cyberspace and making it conducive enough for local and international economic transactions especially in the areas of banking and commerce. Based on the success factors in other countries, and on expert views and opinion, the latter part of the paper equally posits how such efforts would be directed to impact positively in the country's Internet banking development and reduce the prevalence of Nigerian Internet fraud, money laundry and other cross border financial crimes that are linked to Nigeria.

Local Initiatives Against Internet Frauds

Before now, the Nigerian government had adopted various regulatory measures to fight economic and financial crimes in the country. Some of such measures include, among others,

• the promulgation of the National Drug Law Enforcement Agency (NDLEA) Act No. 48 of 1989 – which was sent to confront the menace of money laundering, and to comply with the Vienna Convention;

• the Failed Bank (Recovery of Debt and Financial Malpractice in Banks) Act No. 18 of 1994 – which was promulgated to check the cases of money laundering and insider abuses by bank officials in the country;

• the Money Laundry Act of 1995; the Advanced Fee fraud (419) Act of 1995; and the comprehensive amendments of the Banks and Other Financial Institutions Act (BOFIA) and the Central Bank of Nigeria Act in 2002.

• The Anti-Corruption Act of 1999, which established the Independent and Corrupt Practices and Other Related Offenses Commission.

As argued in the first part of this paper, these laws today look very out-of-place in the present era of Internet banking. Interestingly, the government in recognition of the laspses in the above laws on electronic financial transactions and commerce, has long been occupied with efforts to close such gaps. In 2001, for instance, there was a proposition for the establishment of a National Electronic Commerce Council (NECC) under the Federal Ministry of Science and Technology. The body, which was later dumped in 2003, was expected to serve as the regulatory body for e-commerce and would be made up of professionals from the public and private sector.

At the same time, the Nigerian legislative arm (the National Assembly) has since 2001 been deliberating two bills relating to the Internet and electronic usages – the Internet Freedom bill and the Electronic Data bill. While the Internet Freedom bill is aimed at empowering the government to implement an integrated internet policy that will ensure a vibrant internet culture in the country; the Electronic Data bill is targeted at according electronic data legal effect, validity, admissibility or enforceability. On its own side, the former also proposes an Internet curriculum for the educational institutions to align with global trends by equipping Nigerian students with relevant Internet skills for the global age, while the latter is focused partly on addressing all issues concerning electronic commerce in the country using consistent and environmental friendly regulatory frameworks.

In 2001, the Nigerian government also inaugurated the National Committee on Advance Fee Fraud (NCAFF), and charged the body with the task of formulating the more effective strategy for fighting fraud perpetrators and their agents in the country. This was against the backdrop of the plan by the United States , Britain and France , among others, in November 2001, to sanction Nigeria unless some serious steps were taken to solve the menace of Nigerian financial crimes. A deadline to this effect was given as December 15, 2002. The report of this committee culminated into the passage into law of the Economic and Financial Crimes Bill 2002, which among others established the Economic and Financial Crimes Commission (EFCC). The 19-member Commission was set up specifically to deal with cases of 419 and enforce the various laws relating to banking in Nigeria . Its relevance in the general fight against Internet banking frauds lies in the fact the regulation establishing it gives it unrestricted access to investigate the accounts of bank customers suspected of 419 fraud.

In 2003, a new national body - the Nigerian Cybercrime Working Group (NCWG), was inaugurated under the Chairmanship of the Attorney General of the Federation and Minister of Justice. This new body has since 2004 been working on a project titled “National Cybersecurity Initiative”, which is aimed at developing cyber crime and cyber security regulations in the country. These efforts have culminated into a draft proposal, the “Computer Security and Critical Infrastructure Protection Act”, which is currently waiting to be passed to law by the National Assembly. Some of the intents of the proposed law are to create a central institution (the National Cybercrime Working Group) that will be responsible for the enforcement of its provisions ; and to seek to regulate the security of computer systems and netwworks and protect sensitive ICT instfrastructures (Daily Sun Newspaper, 2004). The new law when promulgated seeks to prohibit three main classes of conduct, namely: (1) Conduct against computer systems, with “Offence in this category made up of activities like unauthorized access to computer systems, access exceeding authorization, computer systems and networks interference, systems intrusion, data interception, denial of service, computer trespass, email bombing, etc.; (2) Conducts utilizing ICT systems to commit unlawful acts or crimes, covering such offences as computer contamination, illegal communications, computer vandalism, cyber-squatting, cyber-terrorism, cyber-pornography, online intellectual property theft, etc.; and (3) Unlawful conduct against critical ICT infrastructures in Nigeria (Daily Sun Newspaper, 2004).

The Nigerian Cyber crime Working Group (NCWG), which is still awaiting legal recognition, is an intergovernmental body. The body has its membership made up of the all key law enforcement, security, intelligence and ICT agencies of government, plus major private organizations in the ICT sector; including Economic and Financial Crimes Commission (EFCC), Nigeria Police Force (NPF); the National Security Adviser (NSA), the Nigerian Communications Commission (NCC); Department of State Services (DSS); National Intelligence Agency (NIA); Nigeria Computer Society (NCS); Nigeria Internet Group (NIG); Internet Services Providers' Association of Nigeria (ISPAN); National Information Technology Development Agency (NITDA), and Individual citizen representing public interest; with its leadership made up of two Chairmen and one Coordinator. The Group is expected to handle cyber crime and cyber security matters and coordinates enforcement, investigation, as well as prosecution, with other law enforcement agencies in the country.

Also in 2003, the Central Bank of Nigeria released the Guidelines on Electronic Banking in Nigeria . The main intent of the guidelines was to define technical requirements and permissible scope of electronic banking, as well as the modalities for adherence by Nigerian banks.

On its own, the EFCC has since 2003 championed some legislative moves for the amendment of the country's Criminal Procedure Law to allow for the easiness of prosecution, for in the words of the Chairman of EFCC, "the legal regime as it is currently couched is prone to manipulation". The Chairman continued that areas being proposed for amendment include “bail, adjournment, spurious motions, unduly long trials and underhand tactics for which lawyers are notorious in employing to delay the legal process ought to have been addressed in the light of the experience of the ICPC, which is yet to secure up to three definite convictions four years after establishment"(Vanguard Newspaper, 2003).

Another Bill, tagged Advance Fee Fraud and other Fraud -related Offences Bill 2005, is also waiting to be passed into law by the National Assembly. The proposed Bill seeks to repeal the Advance Fee Fraud and Other Related Offences Act, and provides among others for a 20-year jail term, without an option of fine, for anyone convicted of 419 and a 10-year term for persons involved in laundering of funds. It also specifies that where a body corporate is convicted of an offence under this bill, the court may order that the body corporate shall thereupon and without any further assurance, but for such order, be wound up and all its assets and properties forfeited to the Federal Government.

Unfortunately, despite the catalytic effects of the spread of Internet fraud, the country is yet to settle on what should be the optimal regulatory instruments and structures.

Global Against Nigerian Internet Fraud

It is very clear now that regulating cyber activities, especially in the areas of economic and financial dealings, can no longer be left only in the hands of national governments and regulators. According to a 2005 Working Paper (document A/Conf.203/7), prepared by Committee I of the Eleventh

United Nations Congress on Crime Prevention and Criminal Justice, there is an urgent need for the UN Information Service Congress to establish mechanisms at the national, regional and international level to improve data collection on economic and financial crimes; devise ways to improve the global legal framework to counter economic and financial crimes; provide effective technical assistance to developing countries to improve their capacity to confront the problem; initiate agreement on measures to improve cooperation between government and the private sector in preventing such crimes; among others. Amplifying this stance, Williams (2002) earlier argued that:

It is now widely recognized that purely national or even bilateral responses are simply inadequate to deal with the problem. The dynamics of illegal markets, the activities of criminal enterprises, the reach of criminal networks, and the pervasiveness of money laundering all militate in favor of multilateral responses. So too does the lack of capacity of weak governments to respond adequately, the unwillingness of corrupt governments to take decisive action against indigenous criminal organizations, and the reluctance of many offshore financial centers and bank secrecy jurisdictions to initiate measures that would keep out the proceeds of crime. Also fueling the growing efforts at governance in this area is the recognition that in some cases, governments themselves are part of the problem. This is not simply a competition between sovereign states and what James Rosenau termed “sovereignty-free actors”; in some cases, state structures and institutions have been neutralized, compromised, or coopted by criminal organizations.

Because of the global nature of Internet transactions, it is now time for countries, especially the economically advanced ones, to focus regulatory efforts not only on the developments within their respective economies, but also on the developments in other weaker economies. This may have explained why in the bid to design necessary regulatory and policy frameworks against international crimes, much focus has been shifted to Nigerian kind of financial and economic crimes (that is the “419 fraud”).

In United States of America, for example, there is currently a working group whose function is to develop policies and plans to combat international Nigerian crime by supporting the task forces; helping to select task force cities and assuring that the task force cities carry out the mission of the NCI; and addressing policy issues, such as privacy and discovery in criminal cases. Also, there is an arrangement on ground tagged ADNET, which serves as a network arrangement on ground for storage and retrieval of data on Nigerian crime. It is part of the duties of the Working Group to educate Internet users on how to effectively apply ADNET.

In 1998, the Attorney General of the US designated the United States Secret Service as the lead investigative agency for Nigerian crime. Through the Secret Service Internet website, and its Financial Crimes Division in its Washington headquarters, the Secret Service acts as a central repository for complaints above Nigeria fraud (Buchanan and Grant, 2001).

Other measures targeted at reducing cyber crime and other related economic and financial crimes, like money laundering involving Nigerians, include the current effort by the FBI in training law enforcement agencies in Nigeria and Ghana . In 2005 for instance, Cyber Division FBI supervisors conducted training in Ghana and Nigeria , and deployed agents to Nigeria for extended temporary duty assignments to actively work with Nigerian law enforcement regarding top targets identified in Operation Relief.

There is also the African Working Party on Information technology Crimes formed under the auspices of Interpol. Ironically though, the body does not presently have Nigerian representation. This is so despite the fact that being part of the party is advantageous to the national government and is capable of enhancing the Internet image of the country overseas. Again, it is one of the requirements for signing up to various international conventions against cybercrime and international financial crimes. Already, there are numerous United Nations conventions the country needs to sign up to in her quest to reposition herself in the global Internet community. One way of practically demonstrating such commitment is to sign up and ensure that the country implements fully all relevant conventions and the Financial Action Task Force recommendations on economic and financial crimes – some of which are the UN Convention against Transnational Organized Crime (adopted on 15 November 2000), the UN Convention against Corruption (opened for signatories in December 2003), the UN Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (adopted on 31 May, 2001), and the UN Convention for the Suppression of the Financing of Terrorism. These conventions are not only capable of providing a disciplined and prudent approach to government decision-making, but also afford the country an opportunity to gain global experiences in Internet regulations and policy.

In addition to signing up to these conventions, there are opportunities for the Nigerian government to go into bilateral agreements with other countries that have strong economic and social tiers with Nigeria . The United States , China , Britain , France and the host of others readily come to mind here. Interestingly, Nigeria is at present a member of a 26-member anti-Spam group called the London Action Plan. There is also the Cybercrime Convention of the European Council adopted in November 2001 as the first major international agreement to regulate on juridical and procedural aspects of investigating and prosecuting cybercrimes, particular as it affects the prevention of illegal intervention into the work of computer systems.

International corporate organizations are also beginning to see the need to assist in this fight. Just recently, the Nigerian government signed an agreement with Microsoft that required their working together to end Internet crimes. According to Neil Holloway (President Microsoft Europe) “it is the first-ever agreement Microsoft has signed with an African country to aid law enforcement efforts. Microsoft's aid will include providing information to law enforcement in addition to training. The company has already been working with Nigerian authorities over the last three to six months. We think we have a responsibility to make an impact in this particular area" (B Blogger, October 21, 2005). Such efforts are commendable and should be emoulated by other multinational corporate organisations.

The Way Forward

Getting the country's economic and social institutions to fully optimize the benefits arising from Internet and be integrated in the global Internet development requires strong political will on the part of government, objective commitment on the part of the private sector, full cooperation on the side of the Nigerian public, as well as an effective collaboration and assistance from the global community. Appreciably, the Internet security policies of major countries such as the United States of America and Britain tend to focus in larger part on how to prevent the incursion of Nigerian cyber-criminals. Apart from preventing the spread of Nigerian Internet frauds internationally, it is important to recognize the indispensable place of the local banking system in the fight against this odd. In the main, the banks are the agents of transferring funds to and from overseas; and the increasing role of electronic and Internet banking is making such transfers easier than usual. Getting things right within the local banking system therefore becomes an option not to be ignored in the whole campaign. This demands, among others, promulgation and objective enforcement of necessary electronic banking laws and policies in line with international standards; effective public education not only on Internet frauds and their regulatory implications, but also on the general applicability of Internet in banking and other forms of financial transactions; adequate funding of the necessary structures (such as the law enforcement agencies and the requisite infrastructure) for the delivery and facilitation of Internet banking; and initiating necessary collaborative strategies for benefiting from the widely publicized global campaign against Nigerian Internet frauds in particular, and the economic and financial crimes in general.

As earlier identified, Nigeria presently lacks the regulatory capacity to control the global spread of Internet fraud and other financial crimes that have roots in the local banking system. Most of the regulations relating to banking and commerce in the country predate the present electronic banking era, and so lack appropriate provisions to achieve an organized and systematic Internet banking development. Even the most recent E-Electronic Banking Guidelines released by the country's Central Bank could not cover this gap. Given this reality on ground, the first major task in the quest for a globally acceptable Internet banking system in the country is the promulgation of requisite laws and policies. Such regulatory framework should be able to address the most important driving forces in Internet banking among customers, which include better access to the services, better prices and higher privacy. It should be guided towards providing the public access to cheap, fast and easy telecommunication services, while at the same time providing banks with adequate legal cover on services provided through the Internet (Ovia, 2001). The regulations and policies must also be such that fully takes into consideration available administrative expertise and resources, as well as political constraints and economic impacts in the country's wider economy (Guasch and Hahn, 1999). As has been argued by Norgren (2001), for instance, there is need to show caution for a too fast and malplaced regulation of a technology that still is developing. That is to say that Internet banking regulation should be made to be adaptive and proactive.

In line with the recommendations of Carlson et al. (2001), regulators must determine the

appropriate balance between meeting set regulatory objectives, avoiding unnecessary costs and distortions that are capable of harming the development of Internet banking and commerce. Such provisions in the E-Banking Guidelines that are inhibitive to electronic banking development can be rebalanced along with reasonable industry discretion or if possible entirely removed from the guidelines. One of such provisions is the case of restricting Internet banking on only naira denominated transactions. This particularly fails to recognize the global nature of this area of banking.

Internet banking laws and policies, no matter how efficient and comprehensive, only make sense in the presence of necessary ICT infrastructural facilities. As has been stressed by Malakata (2005), the growth of e-commerce depends on good communications infrastructure, effective legal and regulatory framework and the development of electronic banking solutions by financial services providers. The attention of government and its relevant agencies is called here, especially as it has to do with reducing the cost of interconnectivity and general ICT access. According to the Global Internet Policy Initiative (2004), for instance, to speed the spread of the Internet in developing countries, the cost of Internet connectivity and bandwidth must be reduced and the quality of service improved. The body recommended the adoption of the Internet Exchange Point (IXP) as one of the most effective mechanisms to accomplish both cost and service gains. According to the body, an IXP is a facility operated by a single entity to facilitate the exchange of Internet traffic between three or more ISPs.

At present, the banks are going through systems integration after the comprehensive industry convergence occasioned by the ongoing banking reforms in the country. The fear here lies in the fact that this process may give rise to system lapses and hence increase the level of frauds. Protecting banks' ICT facilities from experienced bank staff that are likely to be displaced after the integration process is an important issue. This is so considering that internally among these banks, poor recruitment policy, job insecurity and greed among bank staff remain the largest set of incentives for bank frauds. Given the arising difficulties arising from e-banking, banks must also reexamine their recruitment policies as a way of making their cyber banking attractive and protective. It is also important that the Central Bank of Nigeria reviews the prevailing Guidelines on Ethics and Professionalism in Banks, and ensures that defaulting banks and bank staff are penalized accordingly.

At the same time, acquiring software that would be capable of handling the emerging divergences in the system is also a challenging issue. Already, banks have started complaining of the huge cost of integration, with the largest consolidated bank, the United Bank for Africa Plc., indicating that it had already invested as much as N1 billion (about US$8 million) on its systems integration in the last one year. These are indeed important areas for regulatory concerns. The Central Bank of Nigeria would have to ensure that cost is not a hindrance in the needed systems integration among the emerging banks. This is especially so given the fact that most of the applications that were in use prior to consolidation lacked the capacity and scope to match the new trend in the industry, more so in the area of handling complex operations of a mega bank.

Providing infrastructure and acquiring necessary software would also have to be augmented with ensuring that the banking publics have wider access to Internet, if the investment must be meaningful and rewarding to banks. In the developed countries, using public Internet cafés to transact Internet banking and other forms of sensitive financial transactions is practically discouraged. In Nigeria and other developing countries, where access to computer and Internet is in most times available only through commercial providers, it becomes difficult for banks to control the delivery of their services through such terminals (Daily Sun, 2006). This is a very serious problem especially considering the fact that any banking transactions by a customer from public cyber cafés can easily be trailed and cracked by Internet fraudsters. This then leaves the banks with one clear option – that is investing in cafés and having their staff posted to such terminals. Or even having such cafés located within their banking premises, at least as an interim measure.

Today, cyber cafés have become very important means of livelihood to most Nigerian business men and women. The number of cafés in the country is estimated to have grown from a level of about 1800 in 2003 to over 5500 as at December 2005. Ironically, these outfits are not in any way regulated or supervised. In fact, in most cases, what the owners and users use them for does not seen to be the concern of government and regulatory agencies. The effort of the law enforcement agents, where it exists, is mainly not targeted to objectively controlling the activities of the users and operators. In addition, the danger in regulating Internet banking and commerce transactions arises from the fact that the country's ISP's and Cyber café, operate in a highly deregulated Telecommunications Industry, with most of the Internet traffic being routed to VSAT Backbone Providers all around the world (Oyesanye, 2004). This has made cyber activities, not only vulnerable but outside the control of government. Hence,

correcting this trend is expected to be at the forefront of the renewed efforts to instill sanity in the country's cyber highways, since clearly none of the other measures may work out smoothly in such highly risky circumstance. It follows that for effective control of Internet commercial and financial transactions, government may have to put up a supervisory mechanism to ensure that these outfits are not continued to be used as dames for cyber criminals. One way of achieving this is to get the operator of these commercial cyber outfits to install necessary softwares that allow the law enforcement agents to monitor their activities from strategically located terminals. Equally, a lot can be achieved by developing a set of guidelines guiding the establishment, operations and use of commercial Internet centres and ISPs (Internet Service Providers) in the country.

The issue of enforcement should be seen as joint efforts among the governments, the regulatory authorities, the banks and the global stakeholders. Banks in Nigeria, for instance, should note that the growth in Internet banking in countries with great success factors, such as America, Finland, Britain and Japan, was not because of the perfect state of the existing Internet laws in these countries, but more because of the efforts at the individual bank levels to keep customers account safe even where the identities of such customers are cracked or stolen.

Curbing the recklessness of the country's law enforcement agents and garnering strong political willingness on the side of the state and the regulatory authorities remain the best strategies for enforcement of economic and financial laws the world over. There are for instance incessant press reports that police raid commercial cyber cafés, arrest users and force them to pay amounts ranging from US$20 to US$35; and in some cases, the operators are compelled to pay up to US$70 per raid (Oyesanye, 2004). It is important to note that enforcement does not have to be allowed to constrain speed, freedom of time and place – factors that have been found to be major reasons for wider spread of Internet banking in Finland which has one of the highest reputations in cyber-banking growth (Mattila et al., 2001). Instead of the business-as-usual attitude of the Nigerian police, it has been suggested that a special force modeled after the cyber cops operating in several developed countries be set up, with the special squad trained in cyber policing and equipped for the job. The team, alongside other interested parties, should link up with other agencies worldwide to share information and track culprits (Daily Champions Editorial, 2003).

A situation where fraudsters and corrupt individuals are allowed to continue to hold sensitive security offices does not give room for the smooth operation of any law, no matter how well drawn and intended. Example here are the cases of the immediate past Inspector General of the Nigerian Police (convicted of financial frauds), and that of a member of the National Assembly (late Chief Maurice Ibekwe) who as at the time of his arrest for alleged 419 offences was the House Committee Chairman on Security (as well as the House Committee Chairman on Police Affairs between 1999-2003). There are numerous cases of such mix-ups in the country.

Nigeria indeed needs a political structure to fight Internet frauds. There is for instance nothing wrong in having a Cybersecurity Secretariat to advise the Government on issues concerning Internet policies and development. Instituting strong and active body for tracking down regulatory developments from various international groupings is also very pertinent from this perspective. This would allow government to achieve a degree of convergence between the various local regulatory measures and international regulations on different areas of Internet banking. This is one of the ways to reduce the growing disparity in the law enforcement infrastructure between developed and developing countries (Uche, 1998).

It is also important to give the NCWG a legal backing, by facilitating the passage into law the “Computer Security and Critical Infrastructure Protection Act”. This is so because at present, the attention of the EFCC has been diverted towards fighting political corruption, which has reduced its capacity in handling the complexities of Internet fraud. Instead of adopting the business-of-as-usual approach, Nigerian Police and the Economic and Financial Crimes Commission should appreciate the intensity of the growing level of Internet fraud and its damaging impact on the economy. To this effect, a lot local integration of their security network is very necessary. A Police Electronic Crime Laboratory can for instance be jointly instituted, where activities of the Internet hackers and crackers can be easily detected and prevented. More so, such laboratory would have to serve as a databank and a gateway for collaborating with banks, and the reporting suspected cyber criminal cases to the enforcement agents. This would be made to complement the almost dormant Internet Fraud Complaint Centres (IFCC), which already exists in some cities in the country.

Enforcement of relevant Internet banking regulations need to take after the financial disincentive

model not only from the point of view of the banks as contained in a CBN circular on money laundry, but more from the point of view of discouraging individuals from getting involved in the crime. One strong measure here is to intensify enforcements of all rules encouraging the confiscation of assets (both financial and physical assets) of people found guilty of the crime. For now, the EFCC focuses emphasis on arrest and prosecution of suspects, with less emphasis on prevention of the spread of corruption and frauds at all levels. The agency needs, therefore, to be equipped to be able to effectively combine the duties of prosecution and prevention. One of the ways of achieving this is by ensuring that the staff of the commission is well trained and exposed to the sophisticated and internationalized nature of most Internet frauds. An alliance to this effect can be formed with the ever-willing international agencies and governments.

However, for government efforts and resolves in ensuring full enforcement of regulations on Internet banking to be fruitful, certain background socio-economic issues would need also to first be addressed. Enough public pressure from banks and other stakeholders need to be exacted on the Nigerian government to tackle the inordinate cases of poverty in the country. Government should create jobs to enhance the living standards of Nigerians and put the economy back to development track to be able to accommodate the mass of university graduates turned out on annual basis without hopes of getting paid jobs. The social atmosphere as it is today, especially in the light of the devastating short-run effects of the on-going economic reforms, does not equally help matters. More importantly, it has been suggested that to make the on-going economic reforms more meaningful, government ought to provide necessary social safety nets for cushioning the short-term effects of the reforms (Ezeoha, 2005b, p.129).

As stated above, effective public education on Internet banking, Internet frauds and their regulatory implications is also another basic way of handling and controlling the spread of financial crimes on the net. As has been indicated by the US House Committee on Energy and Commerce (2001), a more significant deterrent to cyber fraud and crime is consumer education and awareness; and as our knowledge as on-line users increases, the risk of us being taken by fraudulent activity decreases dramatically. Also, the African Regional Preparatory Meeting for the Eleventh United Nations Congress on Crime Prevention and Criminal Justice, held in Addis Ababa , 1-3 March 2004, recognized public awareness as one of the most important ingredients for fighting the spread of organized crimes. At the same time, a United States House Committee hearing on Online Fraud and Crime, identified that education was needed on an ongoing basis to make consumers aware of the danger signs of fraud and give them confidence in the new electronic marketplace. In the Nigerian setting, education and enlightenment still remains in the main the most important weapon needed for quicker transformation of the citizens orientation and knowledge about Internet usage in the country. One way of going about this is to ensure a wider spread of computer literacy in the country. As was reported in a 2001 Guardian [Nigeria] Editorial, the onus is partly on the government to create an enabling environment for turning computer usage into part of public habit by including computer education in the school curriculum at all levels. At the same time, there are also expert calls for private citizens to be encouraged to join in the awareness programme and donate computers to institutions that need them.

Since 2003 also, ICPC has been working with the Nigerian Educational Research and Development Council (NERDC) to develop an anti-corruption curriculum, which will be infused into subjects at the primary, secondary and tertiary levels of education. These efforts are meaningful only if they are facilitate and allowed to come to limelight in the overall campaign against global crime.

Commissioning expert and intelligent researches on Internet usage in Nigeria , is a clear way the regulatory authorities, international communities and the Nigerian government particularly can assist in the proposed education and enlightenment programmes. Such studies can be tailored to focus on demographic data about Internet users and providers in Nigeria , the purposes of Internet uses in the country, the traffic intensity, and so on.

Funding is also another critical issue in developing and safeguarding Internet banking and commerce in Nigeria . In a United States House Committee hearing on Online Fraud and Crime, for instance, it was suggested among others that part of the ways to make Internet a safe place is to “provide more resources for fighting Internet fraud. Law enforcement agencies need more resources to train investigators and prosecutors and to bring actions that may entail appearing in court in another country ---”. Funding does not necessarily need to come from the government alone. Corporate organizations, especially the banks, the multinational oil companies and other corporate and rich individuals of goodwill should be convinced to get involved in funding institutions, campaigns and other structures for fighting Internet crimes in and around the country.

Finally, to be considered also is the idea of collaboration. Interestingly as identified in a paper titled International Coordination for Cyber Crime and Terrorism in the 21 st Century,

> Some governments recognize that it is not sufficient to address only the local or national aspects of safeguarding information and critical infrastructures. Because attacks against the Internet typically do not require the attacker to be physically present at the site of the attack, the risk of being identified is significantly reduced. Besides the technological challenges this presents, the legal issues involved in pursuing and prosecuting intruders adds a layer of difficulty as they cross multiple geographical and legal boundaries. An effective solution can only come in the form of international collaboration.

The above statement reveals clearly the dangers the international governments and institutions face if no immediate and effective collaborative relationship is initiated with the developing countries on how to curb the spread of cybercrime. According to Udotia (2005), “e volving a truly global culture of cybersecurity means assisting developing economies adopt the technology, processes and people of cybersecurity”; and that it might be of the best interest of the developed countries to initiate the assistance towards building safe cyberspace.

The efforts of the EFCC are yielding some fruits and should be complemented by international law enforcement agencies like the Interpol and the FBI. The effectiveness of the Commission to this effect was tested in August 2005 when it arrested and prosecuted a Nigerian woman charged of defrauding a Brazilian bank of US$242 million. This shows that with adequate support and assistance, the EFCC and the NCWG (when legally instituted) can be good allies to the international community in the global war against 419 frauds and other forms of cybercrime.

CONCLUSION

The above review shows that both local and international efforts on how to eliminate Nigerian Internet fraud and other forms of financial crimes are still evolving. As the Nigerian government battles for an optimal Internet policy framework and regulation, and as major developed countries battle to build walls against the incursion of cyber frauds originating from Nigeria , the need for active collaboration and assistance becomes more glaring. A central focus of these local and international efforts should be the Nigerian banking system. This is so because with the full protection of the banking system, capital flows among cyber criminals and their innocent victims might be discouraged. This capable of creating some forms of disincentive for Internet fraud and financial crimes generally.

References

Awamleh, R.; Evans, J.; and Mahale, A. (2003), *Internet Banking in Emergency Markets: The Case of Jordan – A Note* , Journal of Internet Banking and Commerce, Vol. 8, No. 1.

Buchanan, J. and Grant, A. J. (2001), *Investigating and Prosecuting Nigerian Fraud,* United States Attorneys' Bulletin, November, pp. 39-47.

Carlson, J. Furst K., Lang W. W. and Nolle D. E. (2001), *Internet Banking: Market Development and Regulatory Issues* , Society of Government Economists Conference 2000, Washington D.C., November 17 (http://www.occ.treas.gov/netbank/SGEC2000.pdf)

Central Bank of Nigeria (2003a), *Report of the Technical Committee on Electronic Banking, February.*

Central Bank of Nigeria (2003b), *Guidelines on Electronic Banking in Nigeria ,* August (http://www.cenbank.org/OUT/PUBLICATIONS/BSD/2003/E-BANKING.PDF).

Daily Sun [Nigeria] Newspaper, August 2, 2004

Daily Sun [Nigeria] Newspaper, March 13, 2006

Ezeoha, A. (2005a), *Regulating Internet Banking in Nigeria : Problems and Challenges – Part 1* , Journal of Internet Banking and Commerce, Vol. 10, No. 3, December

_____ (2005b), *Increasing Incidence of Poverty in Nigeria: An Impact Assessment of the Government's Economic Reform Programme* , Journal of Social Development in Africa , Vol. 20 No. 2,

Furst K., Lang W. W. and Nolle D. E. (2000), *Internet Banking: Developments and Prospects* , Economic and Policy Analysis Working Paper 2000-9, September, (http://www.occ.treas.gov/ftp/workpaper/wp2000-9.pdf).

Guasch, J. L. and Hahn, R. W. (1999), *The Costs and Benefits of Regulation: Implications for Developing Countries,* Policy Research Working Papers, The World Bank.

Kerem, K. (2003), *Internet Banking in Estonia* , PRAXIS Center for Policy Studies.

Malakata, M. (2005), *Electronic Banking Prepares the Way for E-Commerce in Zambia* , iConnecT Online (http://www.ftpiicd.org/iconnect/ICT4D_Livelihoods/ZM_Livelihoods_EN.pdf)

Mattila, M.; Karjoluoto, H.; and Pento, T. (2001), *Internet Banking Adoption Factors in Finland ,* Journal of Internet Banking and Commerce, Vol. 6, no. 1

Norgren, C. (2001), *Impact of the Internet in the Functioning and Regulation of Markets* , Public Documents of the XXVI th Annual Conference of the International Organization of Securities Commissions (IOSCO), 23-29 June, Stockholm, Sweden.

Oyesanya, F. (2004a), *Nigeria : Heaven for Terrorist Internet Communication* , The Nigerian Village Square , August 3.

Oyesanya Y (2004b), *Review of Central Bank Guidelines for Electronic Banking* , The Nigerian Village Square, July 13 (http://www.nigeriavillagesquare.com/)

Ovia, J. (2001), *Internet Banking: Practices and Potentials in Nigeria* , A Paper at the Conference Organized by the Institute of Chartered Accountants of Nigeria (ICAN), Lagos, September 5.

Sanusi, J. O. (2003), *Central Bank of Nigeria's Standpoint of Anti-Money Laundering Compliance,* Speech at the Conference on “Anti-Money Laundering in ECOWAS: Bringing the Anti-money Require in Compliance with International Standards, Lagos , June 3.

Singer D. D. ; Ross D. and Avery A. (2005), *The Evolution of Online Banking* , Journal of Internet Banking Business, Number 2 (Spring)

Spong, K. (2000), *Banking Regulation: Its Purposes, Implementation and Effects* , 5 th Edition, Division of Supervision and Risk Management, Federal Reserve Bank of Kansas City.

The Sun [Nigeria] Newspaper, August 2, 2004

ThisDay [Nigeria] Newspaper, December 28, 2004.

Uche, U. C. (1998), *The Adoption of Money Laundering Law in Nigeria* , Journal of Money Laundering Control, January, pp. 220-228

Udotai B. (2005), *Developing Economies and Cybersecurity: Securing the “Weakest Link” of Information Society* , WSIS ITU Thematic Meeting on Cybersecurity, Geneva , June 28 – July 1.

United Nations (2005), *Eleventh UN Congress on Crime Prevention and Criminal Justice* , BKK/CP/08, Committee 1, 2 nd and 3 rd Meetings, Bangkok Thailand , April 19.

Vanguard [Nigeria] Newspaper, December 4, 2003.

Wallsten, S. (2003), *Regulation and Internet Use in Developing Countries,* World Bank Policy Research Paper No. 2979, The World bank Development Research Group, March.

Williams, P. (2002), *Organized Crime and Cyber-Crime: Implications for Business,* CERT Coordination Center .

_____ (1999), *Emerging Issues: Transnational Crime and Its Control, Global Report on Crime and Justice* , ed. Graeme Newman, United Nations Office for Drug Control and Crime Prevention, Oxford University Press.

Wright, J. D. (2002), *Electronic Banking: New Developments and Regulatory Risks* , International Monetary Fund (IMF) Conference – Washington D.C. , May 7-17.