CYBERCRIMES IMPACT ON ELECTRONIC BANKING OPERATIONS: AN APPRAISAL OF THE EXISTING POLICY IN CAMEROON

Written by ***Patricia Asongwe***

Lecturer, Faculty of Laws and Political Sciences, University Of Yaounde 11 Soa, Cameroon

ABSTRACT

Information Communication Technologies (ICTs) revolution has had impacts on almost every aspect of banking operations in Cameroon. However, ICTs have also brought unintended consequences such as criminal activities. Evidence from the existing literature and consultation/ observation indicates that the absence of policy specifically dealing with e-banking crimes in Cameroon has given cyber criminals a loophole to operate freely. This research is especially valuable for the Cameroon e-banking sector, as the findings will provide insights for banks interested in implementing e-banking operations. With the growing threat of cyber criminals, the need for a policy framework to address the menace has become more imperative now than ever before.

Keywords: E-banking, Cameroon, Cybercrimes, Banking, Policy

INTRODUCTION

Although the use of ICTs in banking operations has brought enormous succour to most managers, business executives, financial analysts, and bankers who for long had been yearning for a machine capable of performing complex functions that would considerably result in increased volume of information storage and processing capabilities, efficiency, utilities and transmission and would therefore, catalyse and encourage qualitative and improved services to customers, improved management control and integration for managers, increased operational flexibility and acquisition of new skill, the pervasive and ubiquitous nature of ICTs also have adverse consequences such as criminal activities. [1]

This article specifically assesses e-banking operations in Cameroon and also provides an insight into how cybercrime impacts on E-banking operations from a Cameroonian perspective. The article delves into explaining existing policy, and then evaluates the effectiveness of such policy to fight e-banking crimes.

FROM TRADITIONAL TO ELECTRONIC BANKING OPERATIONS IN CAMEROON

Banking operations have to do with the legal transactions executed by a bank in its daily business, such as providing loans, mortgages and investments, depending on the focus and size of the bank. [2] Otherwise stated, banking operations are the daily transactions of a bank that are legal. According to Section 2 of the 1882 British Bill Of Exchange Act, a banker includes a body of persons whether incorporated or not who carry on the business of banking. This provision lays down a flexible guideline to the activities of a bank. However the difficulty raised by this section, is that of treating the business of banking as being carried on in a uniform manner. This dilemma generally seems to find a solution in the three guiding principles laid down by the courts. Firstly, the courts are open to the fact that the meaning of "banking

[1] Nigudge, S. &Pathan, M. E-banking:Services, Importance in Business, Advantages, Challenges and Adoption in India. Asian Journal of Management Sciences, 2(3), (2014) at 190-192.

[2] Wada F.& G.O. Odulaja. E-Banking and Cyber Crime in Nigeria – A Theoretical Policy Perspective on Causation . Afr J. of Comp & ICTs. Vol 5. No. 1. (2012) at 69-82.

business" can change from time to time. Therefore in *Woods v. Martins Banks Ltd,* [3] the issue as to whether the giving of advice on financial matters constituted banking business. Salmon J. observed: *The limits of a banker's business cannot be laid down as a matter of law. The nature of such a business must in each case be a matter of fact and accordingly cannot be treated as if it were a matter of pure law.* Secondly, the courts hold firmly that, an organisation regarded as engaged in "banking business" in one place may not necessarily be so considered elsewhere. For example in some communities, an institution which accepts deposits of money from the public for the purpose of relending it, carries on banking business, even if it does not open for customers current accounts operation by cheque.

Thirdly, the courts consider an institution's reputation as a matter of great importance. If it is widely considered to be a bank, the courts will be inclined to adopt this view and treat the firm as engaged in banking business.

Article 4(1) of Decree N°90/1469 of 9th November 1990 states that banking operation comprises the reception of deposits from the public, the granting of credits or the putting at the disposal of the customer means of payment, or their management. Additional operations are provided under article 4(2) to cover Exchange transactions (foreign), Investments subscription of shares, purchase, management, custody and sale of stocks and shares and other financial products advice and assistance related to matters of property management, advice and assistance in financial management and in a general manner, all the services designed to facilitate the creation and development of enterprises.

In Cameroon, until 1997, banks were only offering services through the physical branch. It was only in the 1997 that the first e-banking products were introduced. [4]

Accordingly, with the use of new technology, all sectors are introducing a variety of innovative services. Banks offer Internet banking in two main ways. An existing bank with physical offices can establish a Web site and offer Internet banking to its customers as an addition to its traditional delivery channels. From the perspective of banking products and services being

[3] [1958] 3 All ER 166. See also Burke (2002): Electronic Commerce Research and Applications. Business in Cameroon 2014 reports: www.businessincameroon.cm

[4] Mahmoudou, A. (2010). "E-banking support and implementation in Cameroon." Available on www.Camerooninfo.com . Retrieved on the 28th of October 2010.

offered through Internet, electronic banking is nothing more than traditional banking services delivered through an electronic communication backbone, namely, Internet.

AN ASSESSMENT OF E-BANKING OPERATIONS IN CAMEROON

Defining E-banking

E-banking has been defined by a number of authors. This indicates that there is no common agreement on the definition of E banking.

However, for the purpose of this article, e-banking is the provision of retail and small value banking products and services through electronic channels. Such products and services can include deposit-taking, lending, account management, the provision of financial advice, electronic bill payment, and the provision of other electronic payment products and services such as electronic money.

On the other hand, electronic banking can be described as the umbrella term, it is used interchangeably when people refer to one or more forms or components of e-banking such as: Virtual banking, on-line banking, cyber-banking, net banking, interactive-banking, web-banking phone-banking, PC-banking, and remote electronic banking .[5]

Some distinctive features of e-banking

E-banking removes the traditional geographical barriers as it could reach out to customers of different countries / legal jurisdiction. This has raised the question of jurisdiction of law / supervisory system to which such transactions should be subjected,

Secondly, it poses a strategic risk of loss of business to those banks who do not respond in time, to this new technology, being the efficient and cost effective delivery mechanism of banking services,

Thirdly, it is a new form of competition that has emerged both from the existing players and new players of the market who are not strictly banks.

[5]Ayuketang M . N. "Business in Cameroon Impact of Technology on E-Banking; Cameroon Perspectives" Unreported Masters Thesis, Catholic University Institute of Buea (CUIB), (Cameroon, 2016)

Lastly, it has added a new dimension to different kinds of risks traditionally associated with banking, heightening some of them and throwing new risk control challenges,

E-banking Ecosystem in Cameroon

Before the independence of the country in 1960, the banking system in Cameroon was dominated by foreign banks. After independence, foreign financial institutions were French banks, which were there to finance French investments in the country. The existing banks at that time were SCB (Societe Camerounaise des Banques), Credit Lyonnais Group, BICIC (Banque International pour le Commerce et l'industrie du Cameroun), SGBC (SociétéGénérale de Banques du Cameroun), Groupe Société Générale, and la Banque Internationale pour l'Afrique Occidentale au Cameroon (Groupe BIAO).

Various American banks then entered the market, namely Chase Manhattan Bank of Cameroon (Groupe Chase Bank), Boston Bank of Cameroon (Groupe Boston Bank), and the Bank of America (Groupe Bank of America). [6]

Subsequently, the government started to involve itself in foreign banks and acquired partial ownership of BICIC, BIAO, SGBC and Credit Lyonnais. This continued until 1987, when a financial crisis occurred in the country. The crisis resulted in rising prices in Cameroon, trade deficits, and loss of government revenue. It changed the evolution and health of each bank, depending on whether it was a foreign or domestically owned institution. [7]

With the emergence of new technology, all sectors are introducing a variety of innovative services - this is also the case with the banking sector, which is now offering customers a wide range of electronic services.

One of the biggest attractions of Internet as an electronic medium is its openness and freedom. It is a public domain and there is no restriction on who can use it as long as one adheres to its technical parameters. Now, with these changes in the banking environment, the banks are also

[6] [6] See generally Ngafi, D. « Etat des lieux de la microfinace et du système bancaire Camerounais. » Masters thesis Faculte universitaires Catholique de Mons (Belgium ,2006).

[7] Worku, G.. Electronic banking in Ethiopia - practices, opportunities and challenges. *Journal of internet and Commerce*, *15*(2), (2010) at 2-7

offering electronic banking services. [8] As of 2010, 13 out of the 15 banks were offering online financial services[9].[10]

Some Actors Of E-banking in Cameroon

There are Local banks that are involved in e-banking like Mobile Money Cameroon SA, Orange Cameroon and BICEC E-Pay Box.

Some international companies like United Bank of Africa and Afriland First Bank are using I-Card, Virtual Pay Cash and BelCash.

Also, few companies like Globex Cameroon Limited, Wasamundi and Njorku offer the creation of web based businesses with online financial transaction systems for their clients.

Furthermore, telecommunication companies like Orange and MTN Cameroon are now active in the money-transfer business, and insurance companies now issue various bank bonds and guarantees to bank customers.

Another recent innovation in the Cameroon Banking Sector is the introduction of the Western Union system, Express Union and Money Gram, by which systems the transfer of currency from one country to another can be effected even for individuals without bank accounts.

E-banking Techniques in Cameroon

The country now has electronic services, some of which are mentioned here below:

1. *Tele Banking*

Undertaking a host of banking related services including financial transactions from the convenience of customers chosen place anywhere across the GLOBE and any time of day has now been made possible by introducing on-line Tele banking services. By dialling the given Tele banking number through a landline or a mobile from anywhere, the customer can access his account and by following the user-friendly menu, entire banking can be done through

[8] Ibid at 74-75

[9] Worku, G.. Electronic banking in Ethiopia - practices, opportunities and challenges. *Journal of internet and Commerce*, *15*(2), (2010) at 2-7

[10] Nlemba, L. (2008). Electronic cards in Cameroon. Available on www.camerouninfo.com . Accessed on the 21st of february 2018.

Interactive Voice Response (IVR) system. With sufficient numbers of hunting lines made available, customer call will hardly fail. The system is bi-lingual and has the following facilities offered:

• Automatic balance voice out for the default account.

•Balance inquiry and transaction inquiry in all

•Inquiry of all term deposit account

•Statement of account by Fax, e-mail or ordinary mail.

•Cheque book request

•Stop payment which is on-line and instantaneous

2. *Smart card*

A smart card usually contains an embedded 8-bit microprocessor (a kind of computer chip). The microprocessor is under a contact pad on one side of the card. The microprocessor enforces access to the data on the card. The chips in these cards are capable of many kinds of transactions. For example, a person could make purchases from their credit account, debit account or from a stored account value. The enhanced memory and processing capacity of the smart card is many times that of traditional magnetic-stripe cards and can accommodate several different applications on a single card. It can also hold identification information, which means no more shuffling through cards in the wallet to find the right one. Smart cards can also be used with a smart card reader attachment to a personal computer to authenticate a user.

3. *Debit cards*

Debit cards are also known as check cards. Debit cards look like credit cards or ATM (automated teller machine) cards, but operate like cash or a personal check. Debit cards are different from credit cards. While a credit card is a way to "pay later," a debit card is away to "pay now." When you use a debit card, your money is quickly deducted from your checking or savings account. Debit cards are accepted at many locations, including grocery stores, retail stores, gasoline stations, and restaurants. You can use your card anywhere merchants display your card's brand name or logo. They offer an alternative to carrying a check book or cash.

4. *E-Cheque*

An e-Cheque is the electronic version or representation of paper cheque.

The Information and Legal Framework on the E-Cheque is the same as that of the paper cheques.

It can now be used in place of paper cheques to do any and all remote transactions.

An E-cheque work the same way a cheque does, the cheque writer "writes" the e-Cheque using one of many types of electronic devices and "gives" the e-Cheque to the payee electronically. The payee "deposits" the Electronic Cheque receives credit, and the payee's bank "clears" the e-Cheque to the paying bank. The paying bank validates the e-Cheque and then "charges" the check writer's account for the check

5. *Automatic Teller Machine (ATM)*

Plastic money is a new phenomenon in the banking operation in Cameroon[11]. Plastic cards fall into many categories; bank cards including cheques guarantee cards, ATM cards, debit and credit cards. There are other major areas where plastic cards can be used for example, travel and entertainment cards, retail cards, etc. through a combination of printed, embossed and encoded information; plastic cards can perform a number of information. A plastic card can contain information which is printed, embossed or encoded in form of a signature panel or photograph. For greater security in the use of a card, the signature panel can be overprinted. This does not only offer a greater degree of protection against fraud, but also projects a more personalized image. Access to ATM is through the use of Personal Identification Number (PIN) and a plastic Card that contains magnetic strips with which the customer is identified.

With e-banking, people can withdraw money from Automatic Teller Machines (ATM) or pay accounts using a debit/credit card at any time of the day electronic funds transfer (EFT).

It is basically the use of electronic methods or means to transfer money directly from one account to another, rather than carrying cash around or paying by cheque[12]. In 2009, there

[11] First Bank Plc followed suit with the introduction of "FIRST CASH

[12] Dobdinga, C,F.. 'Customer's perception of e-banking adoption in Cameroon: an empirical assessment of an extended" ATM.Dogarawa. (2012) at 124

were only 46 ATMs throughout Cameroon. It should be noted that till now, ATMs are in the main cities, where there are bank branches. In comparison to a country such as South Africa, which has approximately 18 000 ATMs, it is almost as if there are no ATMs in Cameroon. The use of electronic bank cards and the sprouting of Automatic Teller Machines (ATMs) in every nook and cranny of towns and cities is testament to the electronic explosion that grips the entire society , computer usage, Internet usage, telephone usage (NIS, 2010) and electronic banking.

6. *Electronic Funds Transfer at Point of Sale (EFTPOS)*

Electronic Fund Transfer at the Point of Sale is payment that enables a cardholder to pay for goods or service by using a debit card.

7. *Home Banking*

A home banking system usually consists of two parts: a bank computer program and a program in the client‘s computer.

The bank program works as a communication server. It receives calls from clients, verifies their identity, receives data from them, authenticates digital signatures, and generates digital receipts and send data to clients.

8. *Corporate E-banking*

Corporate Electronic Banking (CEB) is a secure internet based service that provides corporate clients with access to online banking it provide the following services; speed in payment processing, access to critical account information for decision making, Access to information such as daily exchange rates for several currencies including major trading currencies, access to reports of all transactions processed by clients through the platform, availability of audit trail information of all user activities, processing of several payments in one bulk remittance transaction.

9. *Financial EDI*

Electronic Data Interchange EDI is the process of exchanging information electronically. EDI enables companies to transmit routine business data such as invoices, product orders, and remittances electronically the purpose of EDI is to speed up the flow of dollars and data EDI is an electronic bridge between banks and customers. It carries detailed trading data alongside

payment information. Traditional paper-intensive communication is no longer cost effective or efficient

10. Netting arrangement

Netting arrangements are an example of electronic data interchange. To illustrate, if Company A buys goods or services from Company B at a cost of 1 million CFA whereas B buys goods or services from A that cost 2 million CFA, then the net flow is 1 million CFA from B to A.

11. *Real-time Electronic (RENTAS*)

Real-time Electronic Transfer of Funds and Securities System provides multi-currency real-time gross settlement of interbank fund transfers, multi-currency debt securities settlement, and depository services for scrip less debt securities and MYR/USD Payment versus Payment (PvP) settlement via USD CHATS (Clearing Housed Automated Transfer System) for its members

12) *Swift*

The Swift network enables users to transmit international payments, statements and other transactions associated with international finance to fellow users. Created initially by banks for banks, the network is now available to approved categories of non- bank institutions which currently include securities brokers and dealers, clearing and depository institutions and recognized exchanges for securities

Benefits of E-banking

As earlier mentioned, the impact of computer and information technology on banking services is tremendous. The system has improved the efficiency of banks and facilitated easy transfer of funds locally and internationally[13]. New money-dealing service based upon sophisticated communication technology has resulted in the introduction of qualitative and integrated banking demands of their customers.

[13] For example Union Bank enables any of its customers to withdraw money from any of its branches irrespective of the branch in which the customers bank.

Modern technology has made it easier for banks to deal directly with each other to communicate and obtain rapid, cheap and widespread information concerning their operations. Also, when our cleaning system is fully automated, it will improve the efficiency of the clearing system, reduce delays and in the long run reduce overhead cost for banks and promote healthy competition among the banks. In practice, effective computerization of banks usually begin with the conversion of information from physical ledger into computer data while updating of customers' accounts is carried out through entering of customer transaction through the keyboard into the computer[14]. Though relatively new in Cameroon, electronic banking has seen customers of commercial banks increasingly becoming receptive. Electronic banking services have provided numerous benefits for both banks and customers and a relevant factor in economic development. The benefits are mentioned below:

- better branding and improved responsiveness to the market. Those banks that offer services such as Internet banking are perceived as leaders in technology implementation.
- new distribution channel providing improved services to customers, as well as the use of electronic commerce strategies.[15]
- improved business efficiency and service quality, and to attract new customers.[16] Technological innovation has been identified as contributing to the distribution channels of banks.[17] Technological innovation has been identified as contributing to the distribution channels of banks. [18] This blend of activities in Cameroon has resulted to a steady move towards detail the varied options in internet services offered by banks. For example; the Carte Visa Electron offers a maximum withdrawal capacity of 250.000 FCFA (US$ 500.00) a day and 500.000 FCFA (US$ 1.000) a week. Other card options offer better opportunities, such as the Carte De Retrait Lion with a maximum withdrawal capacity of US$ 2000(1.000.000FCFA) per day. Cameroon's leading

[14] This system is popularised in Cameroon by Standard Charter, ECOBANK

[15] Rabi, A. Barriers of electronic banking development, case study: Saman Bank. Interdisciplinary journal of contemporary research in Business.3 (5), (2011) at 1-14.

[16] Maiyaki AA, Mokhtar SS. Effects of electronic banking facilities, employment sector and age-group on customers' choice of banks in Nigeria. Journal of *International Banking and Commerce*. 15(1), (2010) at 1-8.

[17] Shanmugam, B. and Supramania, S."E-Banking And Customer Preferences in Malaysia: An Empirical Investigation." *Information Sciences*, (2011)at 207-217.

[18] Ibid. 220

commercial banking giant, BICEC, offers three visa electron cards: BICEC Visa Electron, with a maximum withdrawal capacity of 1.000.000 FCFA (US$ 2.000) a week, BICEC Classic with a withdrawal capacity of 2.500.000 FCFA (US$ 5.000) in just one week and BICEC Gold that provides the opportunity to withdraw up to 5.000.000 FCFA (US$ 10.000) per week, the ECOBANK Card. [19]

- available opportunities for increasing profits. The main objective of every financial organisation is to boost profits for its shareholders, and the Internet offers a potential competitive advantage for banks. As earlier stated, this advantage lies in the areas of cost reduction and increased satisfaction of customer needs.[20] The development of e-banking has greatly helped banks to minimise their overheads, charges and service costs. Many routine services and tasks have now been fully computerised and are quicker and more efficient. The growth of e-banking has made banks more economical, and has also led to the growth of the banking industry, with the introduction of new opportunities for banking processes.
- ensured cheapest distribution channel for standardised bank operations, such as account management and funds transfer.[21]
- The Internet offers a potential competitive advantage for banks - this advantage lies in the areas of cost reduction and increased satisfaction of customer needs

The Internet is the cheapest distribution channel for standardised bank operations, such as account management and funds transfer.

- Through Internet banking, we can check our transactions at any time of the day, and as many times as we want to. Where in a traditional method, we get quarterly statements from the bank. If the fund transfer has to be made outstation, where the bank does not have a branch, the bank would demand outstation charges. Whereas with the help of online banking, it will be absolutely free.

[19] Nlemba, L. Supra note 10.

[20] Bradley, L. & Stewart, K. A Delphi study of the drivers and inhibitors of Internet banking, *The International Journal of Bank Marketing*, *20* (6), (2003) at 250-60.

[21] Polasik & Wisniewski, (2011). Cameroon: financial sector profile. Available on http://www.mfw4a.org/country-focus/cameroon/cameroon-financial-sectorprofile.html . retrieved on the 27th of Ma(Waite & Harrison, 2008:50). Assessed sept 2012.

- Another advantage of Internet banking is that it is cost-effective. Thousands of customers can be dealt with at once. There is no need to have too many clerks and cashiers. The administrative work gets reduced drastically with Internet banking. Expenditures on paper slips, forms and even bank stationery have gone down, which helps raise the profit margin of the bank by a surprisingly large number.
- As far as customers are concerned, their account information is available round the clock, regardless of their location. They can reschedule their future payments from their bank account while sitting thousands of miles away. They can electronically transfer money from their bank accounts or receive money in their bank accounts within seconds.
- One can facilitate payment of electricity and telephone bills, mobile phone, credit card and insurance premium bills as each bank has tie-ups with various utility companies, service providers and insurance companies, across the country. To pay bills, all one need to do is complete a simple one-time registration for each biller. One can also set up standing instructions online to pay his recurring bills, automatically. Generally, the bank does not charge customers for online bill payment.
- funds can be transferred from one account to another of the same or any another bank. Customers can send money anywhere in Cameroon. Once one login to his account, he need to mention the payees's account number, his bank and the branch. The transfer will take place in a day or so, whereas in a traditional method, it takes about three working days.
- With Internet banking, customers can not only pay their credit card bills online but also get a loan on their cards. If one loses his credit card, he can report lost card online.
- One can now open an FD online through funds transfer. Now investors with interlinked demat account and bank account can easily trade in the stock market and the amount will be automatically debited from their respective bank accounts and the shares will be credited in their demat account. Moreover, some banks even give one the facility to purchase mutual funds directly from the online banking system.

Nowadays, most leading banks offer both online banking and demat account. However if one has his

demat account with independent share brokers, then he needs to sign a special form, which will link his two accounts.

Finally, with a range of all kind of products, one can shop online and the payment is also made conveniently through one's account. One can also buy railway and air tickets through Internet banking.

E-BANKING CRIMES IN CAMEROON

E-banking crimes may be referred to as any form of misconduct in cyber space. By definition, cybercrime may be referred to as any form of misconduct in cyber space. It is simply defined as the criminal use of the Internet.

Examples of E-banking Crimes in Cameroon

1) Web defacement

This consists in fraudulently changing the interface of a website; fake profiles on social networks and hacking into emails to con citizens; and using hacked software. Cameroon's place at the top of the Internet fraud list is partly a result of the alphabet.[22] Criminals are taking advantage of Cameroon's Internet suffix ".cm" to trick careless Web surfers who mistype the popular ".com" suffix. By establishing false ".cm" sites that appear similar to the ".com" Web page that people think they are going to, criminals can acquire personal information for identity theft and the spreading of spyware and malicious downloads.[23]

2) Skimming

This is a cybercrime which consists in "hacking magnetic cards with special devices inserted in automatic bank teller machines".

[22] As observed by Defenceweb (2010), Cameroon is home to the world's riskiest Internet sites, according to cybersecurity firm McAfee.
[23] Patricia Asongwe. "A Model Legislative And Regulatory Framework For Cybersecurity In Cameroon." First Commonwealth Telecommunication Organisation Cybersecurity Forum. (London ,2010)

The consequences of "Skimming" on banks are a lesser evil compared to the havoc wreaked by the use of sim boxes in the telecommunication sector. Indeed, this device which enables people abroad to place calls at local tariffs, causes huge financial losses to companies as well as the Treasury.

3) *Phishing*

Phishing is simply a high- tech identity theft that does not only steal personal information and identity from unsuspecting consumers, but also an act of fraud against the legitimate businesses and financial institutions that are victimized by phishing. The most dangerous frauds that causes in day to day banking activity is phishing, a criminal activity using social engineering techniques. Phishers attempt to fraudulently acquire sensitive information, such as usernames, passwords and credit card details, by masquerading as a trustworthy entity in an electronic communication. Very high is the number of phishing attacks against financial institutions, especially banks. What cyber criminals are after are, of course, all types of sensitive information such as account credentials, transfer history etc. A classic phishing attack consists in tricking the user into divulging personal banking data through fake emails. Attackers direct the recipient to a replicated website looking like the real bank site and encourage them to "login" or submit their information via ad hoc forms

4) Pharming

Pharming (from "farming" and "phishing") is based on banks' URL hijacking: when people try to enter their actual bank site, a redirection to another site occurs.

In the unreported case of *The People of Cameroon and UNICS v. Akwosi Theodore, Akenji Valery Claude, Che Ramirez Mundy, and Stanley Tamungong*, the accused was suspected during preliminary investigation for forgery and false pretences punished under section 74, 3 14(1) (2) and 3 18(1) in 2009.The examining magistrate Mme Aminatou Mioum in her forwarding order according to sections 256 and 257 of the Cameroon Criminal Procedure Code before the Court of First Instance charged the above four accused with forgery in banking documents and false pretences due to their regular manipulations over UNICS computer networks and extorting money.

Upon stock taking of accounts, it was discovered that from 24th March 2009, UNICS Banks experienced a lot of transfer orders from her partner HSBC Bank London. It was further noted

that that the accused persons habitually engaged in both banks into transactions which were questionable by nature. Findings therefore, made it clear that the cheques on the 24th and 26th March related to 1,298,500, 3,030,000 CFA francs and 2.100.000 francs CFA emanating from fake international transfers. However, in the course of the sixth reception order, of 2,013,000 CFA francs sent from London Akwosi Theodore Akwo and Che Ramirez were picked up by the General Direction of External Research and were further detained.

Notwithstanding the classification of the learned judge as forgery and false pretence, sanctioned under the penal code, sections 74, 314(1)(2) and 318(1), this was a typical example of an e-banking crime :

5) *Credit card redirection*

Another facet usually exploited by cyber criminals to disturb the smooth functioning of e-banking operations and prevent them from meeting their obligations is through online credit card fraud. In this way, cyber criminals fraudulently obtain the credit card numbers of owner and use them to issue out cheques on behalf of their owner without their consent and knowledge. It is result of this that most hanks today have placed strict restrictions on the amounts that can be withdrawn online by their clients.

6) *Spam*

Spam is an unwanted mail or information or message or it is like a electronic junk mail. Actually these mails or messages will be kept on being sent to your account. These messages or mails will be varying but they are very commercial and their sheer volume also will keep on varying. In these messages they will tell you to buy a product or they may persuade to buy a product or service. They will tell you to visit their web sites where purchases will be going on. When we are doing purchases, they will try to get our personal online banking account details or credit card details.

EFFECTS OF E- BANKING CRIMES

Crimes represent a major concern for e- banking in Cameroon. To emphasize on the severity and the hazardous nature of cyber threats in e-banking, the Director General of the National Agency for Information and Communication Technologies (ANTIC) zoomed-in on common

e-banking crimes perpetrated in Cameroon as follows: Internet Scamming, (1400 cases investigated)-Phishing, (2000 cases investigated)-Identity theft: blackmail or extort money, (1500 cases reported)[24]

The Director General went on to state that local banks lost at least CFA3 billion (more than $5 million).[25] This is an indication that banks in Cameroon suffer enormously from the whims and caprices of cyber criminals. By this means, the criminals obtain illegal access into the official data base of these banks and obtain secret information which is further used to either effect fraudulent withdrawals from clients' accounts. Also, through hacking, these criminals obtain the secret bank codes by inserting a configured magic Sim card that has the capacity to magnet certain sensitive data from the bank's machines. Such information can further be used by them to realize gains in diverse respects. By so doing, this places the e-banking users in a situation of conflict which leads the latter to lose confidence in the former hence, hampering the smooth functioning of banking transactions.

These online misconducts do not only have an adverse effect on the economic growth of Cameroon but may have a negative impact on trust and confidence and consequently hinder e-banking.[26]

E-BANKING POLICY IN CAMEROON

This includes the institutional and instrumental policy.

E- Banking Regulatory Organs

On the regulation/supervisory front for the implementation and enforcement of its decisions are the following:

- The Ministry of Finance which controls all banking activities especially the terms and conditions for banking services. It also receives applications for licensing.

[24] Business in Cameroon In Cyber-criminality wreaking havoc in Cameroon
[25] . Patricia Asongwe, "e-Government and the Cameroon Cybersecurity Legislation 2010: Opportunities and Challenges" The African Journal of Information & Communication (2012) at 159
[26] Nor, K. & Pearson, J.M. (2007). The Influence of Trust On Internet Banking Acceptance. *Journal of Internet Banking and Commerce, 12*(2) at 1-10.

- the regional regulator, COBAC whose supervisory mandate covers the other five CEMAC countries
- BEAC which is the sole central bank for the six countries and have operational branches in each of the six member countries[27]

Other organs are;

- The local financial intelligence unit ANIF (National Agency for Financial Investigation). This has successively within the last three years given us an excellent rating on compliance.
- the Business Coalition against Corruption (BCAC), which is a strong private-sector initiative to combat bribery and corruption in all of its facets.
- the National Credit Council (NCC)
- the Banking and Credit/Finance Association. (APECAM)
- the Telecommunication Regulatory Board (TRB) of Cameroon has as one of its missions the protection of consumers of ICTs protects .This mission can be extended to consumers of e-banking products.
- the courts

Regulatory Instruments

While electronic banking is improving, the law has been slow in protecting customers in electronic banking. There is presently no law that is specific to e-banking crimes in Cameroon. [28] However, this is not to say that e-banking criminals are free to operate in the country. There are general laws that are not specifically related to e-banking crimes but are being enforced to deal with such crimes. Some of these laws are:

I) International conventions, customs law, ordinances, presidential decrees, ministerial orders, circulars and court decisions OHADA facilitate paper based transactions which apparently are not applicable to technological changes that are currently taking place in Cameroon. The existing laws facilitate paper based transactions and are not adequate for crimes taking place in cyber space in Cameroon. These regulatory instruments are flexible in character, which

[27] National institute of Statistics. (2009). *The Cameroonian annual report of statistics indices.* Retrieved from www.BEAC.com on 15 October 2017.

[28] Asongwe P. Supra note 25

means that they can be modified in accordance with socio-cultural, political and economic developments within Cameroon.

There are other laws that are not specifically related to e-banking but can being enforced to deal with the crime.

Other statutes that govern banking industry in Cameroon are here below highlighted.

The Cameroon Penal Code

In Cameroon, the penal code criminalizes offences relating to forgery, theft, misappropriation, false accounting and obtaining by false pretences. The Cameroon Penal Code criminalizes any type of stealing of funds in whatever form, an offence punishable under the Penal Code. Although cybercrime is not mentioned in the Penal Code, it is a type of stealing punishable under the penal code. The most renowned provision of the Penal Code is section 318, which deals with "obtaining Property by false pretences- Cheating." [29] Although the Act outlines property capable of being stolen, the definition is wide enough to cover the theft of physical objects like hardware, floppy disks, programs where it could be shown that the owner will be permanently deprived of it.

Also, this provision can be applied directly, if the perpetrator uses computer device to misappropriate or convert tangible property such as cash, cheques and inventory.[30]The same conclusion would not be reached, however, where a legitimate holder of a bank credit card, through hacking or other devices, withdraws money in excess of his bank's credit. Could it be said that the customer takes such cash against the bank's wish or he deprives the bank permanently of the property? The difficult in applying his provision is illustrated in the case of *R.V. Kassim*[31]and *R.v. Nwabi* .[32] In cases, the accused persons opened bank accounts under false names and addresses and thereafter used the cheque books and credit cards to withdraw cash in excess of their bank balances. They were charged under section 20 (2) of the theft Act, 1968(UK) for procuring the execution of a valuable security by deception. The court held that the accused persons were not guilty of theft under section 20(2), because the credit card did not

[29] See section 314 – 317 of Cameroon's Penal Code; see Carlson Anyangwe. *Criminal Law In Cameroon ;Specific Offences* (Langaa *RPCIG Cameroon 2011) at 155*.

[30] *R.V. Thompson* (1978) 3 AER 216.
[31] 1991) 3 WLR 216.
[32] (1986) 83 Cr. App. R. 271.

constitute security under the Act. The court said that the acts which might find conviction under the Act were those done to or in connection with bill of exchange or other negotiable instrument, including making, acceptance, endorsement, alteration, cancellation or destruction', each of which constituted an execution an execution within the meaning of the act.

The import of these decisions is that a credit card does not amount to security or negotiable instrument within the meaning of the Theft Act, 1968(U.K). It is submitted that the decision were wrongly decided as the court sacrificed justice at the altar of technicality, because ample evidence abound to show act of concession and intention to deprive the bank permanently of cash. It is immaterial that the fraud was committed through computer device.

Difficulties will also arise where information stored in a computer system is taken, interfered with, memorized or photographed by hackers or read without the removal of any physical and tangible objects form the computer system in which the confidential information is stored. In order words, does information constituter property capable of being stolen? The courts has in *Oxford v.Moss*[33]held that information is not property for the purpose of the Theft Act and could not be stolen since the owner is not deprived permanently of the intangible asset. However, a radical approach introduced in a Canadian case *R.v Scallen*[34] where the Court of Appeal in construing section 283 (1) of the Canadian Criminal Code, which is to the effect that, "anything whether animate or inanimate" is capable of being stolen, held that "anything" need not be tangible or material and included a bank credit was truncated by the decision in *R.v. Stewart*[35]where the majority of the court of Appeal held that information is a property incapable of being stolen. But in the U.S case of *U.S. v. Bottone*[36] the court took a different decision and ruled that information copied from computer, even though through secondary means, is a property capable of being stolen. In that case, the defendant was defendant was alleged to have made copies of certain documents without any tangible property being taken at all. The court accordingly had to address the question whether the information contained in the documents per se could be stolen and transported as charged. Having established that the originals of the documents would qualify as valuable goods the court then had to determine whether more

[33] (1978) 68 Cr. App. 183; See also Rank Film Distributors Ltd V. Video Information Centre (1982) A.C. 380
[34] (1974) 4 WWR 345
[35] (149) D.L.R. (3d) 583 (CA); 5 CCC (3d) 481.
[36] 36 USC 389 (1966).

copies of the documents were "goods" which had been stolen, converted or taken by fraud. In holding the accused guilty the court ruled that:

Where the physical form of the stolen goods is secondary in every respect to the matter recorded in them, the transformation of the information in the stolen papers into a tangible objects never possessed by the original owner should be deemed immaterial. The object of the traditional criminal law is the protection of tangible, physical and visible objects as against intangible objects. It is doubtful whether the existing criminal law could cope with the exigencies of e-banking crimes which expand not only the object but introduces sophistication in its perpetration. In considering *therefore, the capacity of the traditional criminal law to cope with these offences, there are three aspects of that law which must be closely examined. One is the distinction made by law between offence of stealing on the one hand and fraud or deception on the other, depending upon whether the property concerned id parted with "voluntarily". The second difficulty involves the treatment of information as "property".*

Cameroon's Cyber Code [37]

The Cyber Code provides the duty of confidentiality by the employee or any member of employee to keep the confidentiality of the licensee information and should not disclose the information to the public or to any other person unless where there an order of the court to do so for security purpose or the information needed by the court as evidence.[38] Accordingly section 41 of the Cyber Code states that "every individual shall have the right to the protection of their privacy." This section also gives the judges the right to take any protective measures notably, sequestration or seizure to avoid or end the invasion of privacy. Accordingly, the law provides for the responsibility of content provider for data transmission, for bidding a natural person or corporate body to listen, intercept and store communications and the traffic data related thereto, or to subject them to any other means of interception or monitoring without the consent of the users concerned, save where such person is so authorised legally.

Stricter security requirements are imposed on the companies whose systems are included in the critical infrastructure, without neglecting owners of other information systems. In addition, the

[37] Law n°2010/012 of December 21st 2010 on Cyber security and Cyber criminality amended and supplemented by Law No 2015/006 of 20 April 2015 on electronic communication.

[38] Nick Nykodym and Robert Taylor "The World's Current Legislative Efforts against Cyber Crime" Computer Law and Security Report, vol, 20(5) (2004), at 398-41

private sector's information security safeguards are increased to provide high security for all information systems.

The Cyber Code therefore serves as the basis for defining the general requirements of an information infrastructure including e-banking by ensuring that the obligations of the state and the private sector in securing information and network infrastructure are specified. As the security of networks largely depend on end-users' awareness of protecting their computers and their capability to do so, the obligations for such users also need to be specified.

Standards in security activities provides a broad field of endeavour aimed at implementing and improving the protection of information and information systems from unauthorised access, use, disclosure, disruption, modification, or destruction. This ensures the authenticity; confidentiality, and availability of information.[39]

Secondly, the Cyber Code also spells out the role of ISPs and other private sector companies that are important in fighting e-banking crimes as follows:

- Data storage

Due to the volume of traffic passing across their networks, it is infeasible for ISPs to keep a complete record of all traffic. The law provides for sophisticated internet surveillance systems, but the technological limitations of gathering and analysing huge volumes of data can be challenging. Logging of less detailed information (such as IP addresses assigned to individual users at particular times) can occur over long periods of time. ISPs generally have the ability to undertake targeted "real-time monitoring" of data, which is important in the investigation of cybercrimes

With respect to the contribution of ISPs to cybercrime prevention, data protection laws can have a number of effects. Data processing restrictions should not in general (at least where sufficient legal exceptions exist) prohibits lawful access to ISP customer data by law enforcement for investigative purposes. A typical exception is that "a non-law enforcement entity" (including a company) that holds personal information is permitted to disclose the

[39] See section 9 of the Cyber Code

information to a law enforcement agency without breaching where it is "reasonably necessary" (for the enforcement of the criminal law. [40]

- Data-Breach Notification

A breach is generally an impermissible use or disclosure under the privacy rule that compromises the security or privacy of the user. An impermissible use or disclosure of unsecured information is presumed to be a breach unless the notification demonstrates (based on a risk assessment) that there is a low probability that the information has been compromised. Thus when a breach occurs, the rule requires in practice to notify affected individuals.[41]

Accordingly, ISPs are required to provide the Agency with the following: reports and information about cyber incidents, threats, and vulnerabilities affecting civilian information systems and critical infrastructure systems; cyber incident detection, analysis, mitigation, and response information; and cyber threat information received by such agencies. The law demands that in the event a private vendor product or service of such an agency is implicated, to first notify such private vendor of vulnerability before further disclosing such information.

Data breaches involving unauthorised acquisition or access of personally identifiable information should be notified to the agency without unreasonable delay after discovery of the breach and potential victims. Based on the risk of harm and consistent with the needs of law enforcement.

Notification is intended to enable victims of breaches to take measures to reduce the security impact (such as changing passwords or PINs, or asking for payment cards to be reissued); to increase the competitive pressure on businesses to improve their security; and to support the work of regulators responsible for data protection and critical infrastructure protection. This requires notification to victims and other responses after data breaches involving personal or

[40] Waite, K. & Harrison, T." Consumer expectations of online information provided by bank Web sites." Journal of Financial Services Marketing, 6(4) (2008) at 48

[41] Longe, O.B & Chiemeke, S.C. "Beyond Web Intermediaries: Framework for Protecting Web Contents on Clients Systems." Paper Presented at the International Conference of the International Association of Engineers IAENG) Imperial (2007) at 166

financial information of individuals. One example of the problems posed by the absence of control instruments is the ability of users to circumvent filter technology

The significance of breach notification rule is that breaches are investigated and penalties may be imposed for failure to comply with the Rules.

- Due Diligence

As per section 40 intermediary shall not be liable for any third party information hosted by him, if his function is limited to providing access to a communication system over which information made available by third parties is transmitted, and if he observes due diligence and follows the guidelines prescribed by the Government.

Thirdly, the Cyber Code prohibits the following:

- Unauthorized access to a computer or intentionally causes or knowingly causes loss or damage to the public or any person, destroy or Section 68 of Cameroon Cyber Code
- Infringement of personal privacy in section 80.

The law further states in section 81 (new) (1) that whoever uses an electromagnetic, acoustic, mechanical or any other device wilfully to intercept a private message and divulge he shall be punished with the penalties provided for in Section 80 . [42] Sections and 37 of the law places liability on physical or corporate person providing certification and electronic signatures. Thus these provision place standards on the use of electronic signature in E-commerce. This in a mechanism to prevent online crime.

Also, the law in its section 41 to 46 provides for sanctions and fines for any misconduct or offence relating to e-commerce

Law n° 2010/021 of December 21st 2010 governing electronic commerce in Cameroon

This law governs electronic commerce in Cameroon. According to section 2, electronic commerce is the production and exchange of goods and service by the use of ICTs.[43]

Sections 36 and 37 places liability on physical or corporate bodies that provide certificate and electronic signatures for failure to prevent users from any danger. The also provide for fines

[42] See also sections 81 – 83 of the Cyber Code
[43] See section 15 of the Law on Electronic Commerce

and sanctions in its sections 41 to 46 for misconducts carried out in e-commerce transaction. These provisions can also be applied to e- banking operations

Consumer Protection Law No. 2011/012

The Consumer Protection Law No. 2011/012 establishes the legal framework for consumer protection in country. This law applies to all transactions relating to the supply, distribution, sale and exchange of technology, goods and services relating to consumer protection. These transactions include health, pharmacy, food, water, housing, educating, financial services, and banking, transport, energy, and communication sectors. [44]

This law protects the rights of consumers in Cameroon and is applicable to banking services as well. Currently, the rights and liabilities of customers availing of Internet banking services are being determined by bilateral agreements between the banks and customers. It is open to debate whether any bilateral agreement defining customers rights and liabilities, which are adverse to consumers than what is enjoyed by them in the traditional banking scenario will be legally tenable. Considering the banking practice and rights enjoyed by customers in traditional banking, it appears the banks providing e-banking may not absolve themselves from liability to the customers on account of unauthorized transfer through hacking. Similar position may obtain in case of denial of service.

APPRAISAL AND THE WAY FORWARD FOR EXISTING POLICY ON E-BANKING CRIMES

It is undoubtedly clear from the analysis above that Cameroon's existing policy is inadequate to grapple with the wave of e-banking crimes.

The Lack of a fully operational legal and regulatory framework jeopardize the security of consumers of E-banking products and cause financial loss particularly in electronic services that involve monies like ATMs, mobile banking, internet purchase of goods and other

[44] Patricia Asongwe "Cyber security and Challenges of Cyber criminality: Response, Strengths and Weaknesses of Cameroonian Law" Ph .D Dissertation, University of Yaounde II, (Yaounde, 2017) at 450-457

payment.[45] As earlier stated, the legal gap that exists in banking laws provides loopholes for offenders to commit offences and also put the users in to risks.[46]

Secondly, there can be uncertainty about which legislation applies to E-banking transactions; the legislation of the jurisdiction in which the virtual bank is licensed or in which the services are offered. This is especially true when E-banking has a cross-border nature where different legislations might conflict with each other. [47]

Thirdly, enforcement of certain emerging areas of law is uncertain, for example laws related to E-contracts and digital signature. This lead to violations of customer‘s protection laws, including data collection and privacy, and regulations for soliciting could be important issues. In other word the author is of the view that customers can only be protected clearly by a system of law.
It can be concluded that this menace of cybercrime has eaten deep into the fabrics of our society and poses threats to the socio-economic development of the country.

Inadequate measure to prevent banking fraud is the primary reason for widespread frauds.

While the e- banking industry in Cameroon has witnessed a steady growth in its total business and profits, the amount involved in e-bank crimes has also been on the rise. This unhealthy development in the e-banking sector produces not only losses to the banks but also affects their credibility adversely.

Recently,

Accordingly this article recommends the following:

- a comprehensive legal framework on information and data protection laws relating to electronic banking must be enacted. The development of proper e-legislation is viewed as being crucial to the adoption of e-banking, since the absence of this would inevitably discourage people and businesses from going online. Security in electronic banking services is greater than that in conventional banking services and requires more specific

[45] Mahmoudou, A. (2010). “E-banking support and implementation in Cameroon.” Available on www.Camerooninfo.com . Retrieved on the 28th of October 2010.

[46] ibid
[47] ibid

attention by bank management. [48]The security of information may be one of the biggest concerns to Internet users. Economic and technological phenomena such as downsizing, outsourcing, distributed architecture, client/server and e-banking all have the goal of making organisations leaner and more efficient.

- an amendment of Cameroon's Criminal Procedure Code or the enactment of new procedural law to fit the digital environment. It is important to understand that criminal investigation requires specific skill sets like forensic accounting and technology to collect adequate evidence. [49] While the evidence unearthed by criminal investigation can vary on a case-to-case basis; typically, it needs to be relevant and comprehensive to be admissible in a court of law. Accordingly, it is suggested that certain additional aspects, such as, the source of the evidence, a legitimate witness, electronic evidence and data should be taken into account in order to add credibility to the case. In the absence of these, banks may not have the confidence to take legal recourse or action.
- enhancement of security procedures like certification, digital signatures, monitoring and authentication as a solution . So, too the enhancement of proactive prevention, and more unique layers of defence to protect what the banks value.
- aggressive public sensitization against cybercrime using the mass media and a platforms for information sharing.
- training of e-banking security experts while ensuring the capacity building for existing bank officials , law enforcement agencies, intelligence agencies and security agencies.
- designing proactive and effective strategies to fight e-banking crimes by the Telecommunication Regulatory Board (TRB) which is the organ in charge of ICTs Consumers' protection in Cameroon.
- best practice by consumers such as not disclosing to strangers personal effects and banking details such as credit card pins, bank account numbers, e-mail codes and use of antivirus on their systems against malware etcetera.
- Last, but not the least, collaboration between all stakeholders e-banking to develop a truly effective crime prevention.

[48] Boateng R. Longe O, and Mbarika V. "Cybercrime And Criminality In Ghana; Its Forms And Implication." Proceedings of The Sixteenth America's Conference On Information Technology (2010) at 135
[49] Asongwe P. Supra 43 at 450

Although banks cannot be 100% secure against unknown threats, we are however hopeful that with the help of these recommendations, e-banking crimes would be able to minimize, customer trust and confidence would be enhanced.