



# ***BANKING AND FINANCE LAW***

1-09-14

Volume 1

## **EDITOR'S NOTE**

In this quarter's newsletter we take a look at Banking and Financelaw, highlighting the current developments and various issues in the sector with special emphasis on the situation in Nigeria.

On the 30<sup>th</sup> of June, 2014 the Central Bank of Nigeria (CBN) rolled out a circular to all Nigerian deposit money banks, development finance institutions, and the Asset Management Corporation of Nigeria on the prohibition of loan defaulters from further access to credit facilities in the Nigerian banking system.

Its content exposed the fact that if allowed to continue, the constant impunity with which borrowers default on their loans, and are yet allowed access to more loans by other banks under the same or a different identity, would eventually result in a plethora of non-performing loans, thereby negatively impacting the liquidity of and creating instability in the sector.

The CBN therefore gave a directive there in, that it is mandatory for all the relevant institutions to carry out credit check on potential borrowers, and to not give out loans to a borrower who is in default of any existing credit facility, to the amount of five hundred million in the case of deposit banks, and two hundred and fifty million in the case of development banks and banks in liquidation except with the prior written consent of CBN. Furthermore the circular provides for a sanction, consisting of payment of 150 % of the sum of the credit facility by any defaulting deposit money bank and their likes.

Another pleasant development in the Nigerian Banking industry is the fact that Entrepreneurs can now access credit facilities/loans from participating financial institutions at an interest rate of 9%.

On the 22<sup>nd</sup> of July 2014, the CBN announced its review of the prevalent interest rate from 21% to 9%, stating that on each disbursed loan, it would receive 3%, equally promising, is the fact that the loan amortization can now be spread over five years, and a minimum of one year within which a bank could demand full repayment.

This is a much welcomed directive that will boost the Nigerian Economy.

Finally, the CBN has resumed the collection of a N65 charge/fee from cardholders' on every 4th Automated Teller Machine (ATM) withdrawal on another bank's ATM, that is other than that of the cardholder's issuing bank, in a month. The first 3 withdrawals monthly are free.

The Central Bank in making these changes has taken into consideration the cost to the bank in deploying and maintaining an ATM. The N65 fee is paid to the acquiring bank (the bank which owns the ATM), and the switching company and is used to cover the costs of the switching, ATM monitoring and processing by the acquiring bank. All withdrawals on the ATM of the cardholder's issuing bank remains free.

Do have a pleasant read.

## SAFETY OF TRANSACTIONS IN ELECTRONIC BANKING

In Nigeria there are no laws governing electronic commerce/electronic banking, however the practice of other jurisdictions such as the United Kingdom, is being applied in the Nigerian Banking Sector.

One can enter into a banking contract via the internet, with the homepage of a banks website being an "invitation to treat", the customer being the one who makes an offer and the bank website content owner being the one who decides whether or not to accept the offer.

It is an implied term in online banking contracts that a customer checks his email at least once a day, mails are considered to be recallable during business hours of the day they have been sent, and considered to be received on the day after the day they were sent.

It should be an express term of online banking contracts that the provider/content owner informs the customer of the risk of fraud and forgery. An example of such a term could be "The client accepts to give orders and have them dealt with via email. The client has been explicitly informed that email and online contracts/transactions are subject to abuse, and as such the provider is discharged from liability resulting from an abuse or misuse of the transmission system".

Furthermore it should be stated expressly with clear remarks that the banks email addresses either, only serve for the transmission of information, and not for transactions/placing orders or giving instructions or it serves for actual settlement of orders, in the latter case such email should be checked regularly by the bank several times a day. The bank should also have a clause in terms and conditions section of its website stating that there is a risk of forgery in email transactions/transmission, an example is "If the client uses email to make and deal with orders, it must be aware that abuses cannot be prevented, the provider/bank is therefore completely discharged from liability that may result from an abuse of the transmission system".

The reality of possibility of input errors in online banking has resulted in the prevalent use of "Confirmation Fields". These confirmation field show the bank customer/ online banking user, the text he/she has entered, to give an opportunity for correction, if needed.

One of the challenges to online banking is the written form required for contracts such as loan agreements, sale of land contracts, surety ship declarations etc. Considering the fact that it isn't encouraging for valid conclusion of online contracts to fail due to legal form requirements, it is suggested by the writer that embedded in the proposed bills on electronic commerce, that there be clause which state that the fact that a contract has been made electronically should not lead to its invalidity.

Consequently, in online banking terms and conditions agreements, it should be expressly stated that the customer accepts the probative value of electronic documents as documentary evidence, with the understanding that the question of the probative value of digital documents will still largely be a matter of the discretion of the court/judge.

It goes without saying that an authentic online banking site must clearly show the name of the service provider, the geographical address, email address and registered trade number (RC number) number of the service provider. Proper details of price of transactions that is whether subject to tax/delivery costs etc., should also be readily available on the site.

In addition, due to the banks duty to provide information, disclosure and advice, must emails contain clauses stating for instance that "This email message is confidential and may contain legally privileged information, if you are not the intended recipient, you should not read, copy, distribute, or otherwise use the information in this email. This email may be susceptible to data corruption, interception and unauthorized amendment, and we do not accept liability for any such corruption, interception or amendment or consequences

thereof. Please telephone or fax us immediately and delete the message from your system”.

As relates to disclosure, the bank has a duty to inform its customers about foreseeable system failures, interruptions by scheduled maintenance services and so on, while the customer has a corresponding obligation to inform the bank of any loss of ATM, PIN code, and any change in sensitive personal details. Most times clauses such as “ the customer is obligated to keep the password and authorization codes secret and to prevent their misuse by unauthorized persons, in particular, after it has been changed, the password must not be written down or stored on the customer’s computer without protection. The customer bears the consequences of any risk arising from the disclosure of PIN codes and other authorization passwords.”

Finally the terms and conditions of the online banking contract must be provided to the customer in a way that allows for storage and reproduction. The customer should also be advised to give special care to the PIN code, bank secrecy and other sensitive data.

Online banking has really taken great strides, for instance, it is now possible to open a bank account on Facebook, the latter being a social media website, see [www.facebook.com/gtbank](http://www.facebook.com/gtbank). The process is simply log into your Facebook account, Go to GTbank Facebook page at facebook.com/gtbank, Click on the Open an account link, Select an account type e.g. GTCrea8, GTSave, Current or others, Enter your email address and your location, Click on continue, Allow GTBank to access your profile when the popup windows comes on, Confirm your personal details, Click on continue, Submit your registration, Print or Make a note of you transaction code(TC), Complete your registration at any bank branch after 2 weeks using your TC.

After you are through with the online registration at Facebook, wait for two weeks and then visit your bank to complete the process using the following: Proof of address: PHCN bill, Water bill or other recent utility bill, Personal identification: Driver's license, student id, international passport, 2 passport photographs, Transaction code.

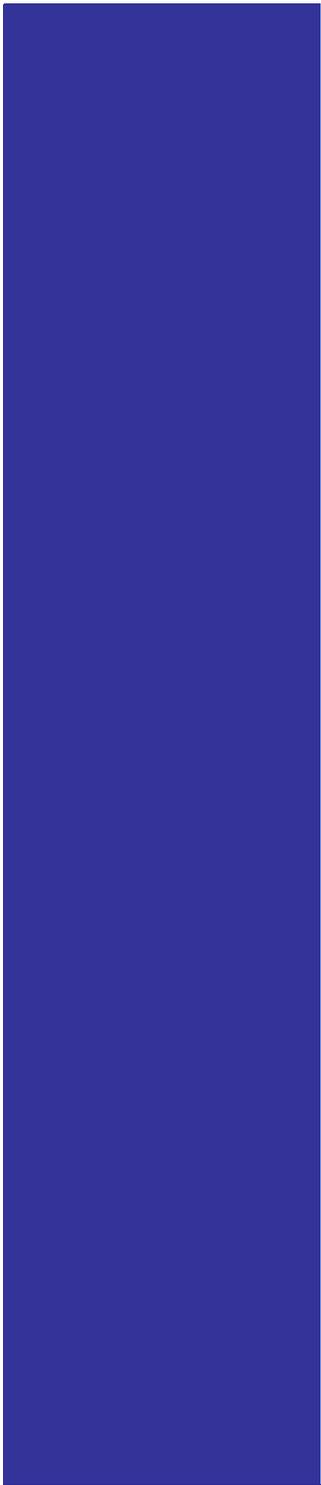
Once you provide your transaction code to the customer service personnel, he/she would be able to quickly access the details you've already submitted on Facebook and this would speed up your account opening process.

The downside of most online banking is that the associated risk is often borne by the customer, who is held liable despite the fact that he is the one suffering damage. Therefore it is common to see clauses that allocate the risk of internet use for banking, to the customer based on the logic that the customer’s computer is the weak link in online banking.

It is expected however as technology advances that there will be a just distribution of risk, as is prevalent in advanced countries, where for instance the credit card issuer is obliged to refund 50% of money lost by a customer due to online credit card fraud or misuse of passwords.

One of the ways for a customer to ensure safety in its online banking transactions is to make sure he/she personally enters the full URL or website address of its bank, rather than clicking on a link embedded on an email supposedly sent by the bank, as some online fraudsters have cloned bank sites, using them to get access to customers password and ATM card PIN codes.

Finally a secure website most times has the sign of “https” preceding the web address, a shady website on the other hand may just read “http”. Despite the risks however, the ease of online banking has done away with the phobia, and besides the courts are ever ready to ensure justice is done in the event of a breach of either the customer or the bank’s contractual right.



## Banking and Finance Law



The GOS Newsletter has been prepared for clients and professional colleagues, it is not meant to substitute legal advice. Please let us know if you would like to discuss any issue in more detail; E-mail: [b.sodipo@gosodipo.com](mailto:b.sodipo@gosodipo.com)  
Copyright © 2014 G.O Sodipo & Co, All rights reserved.

