



09-61638445 (Fax)
09-46238445

CENTRAL BANK OF NIGERIA
Central Business District
P.M.B. 0187
Garki, Abuja

August 30, 2010

REF: BPS/DIR/CIR/2010/GEN/01/169

TO: ALL DEPOSIT MONEY BANKS (DMBs)

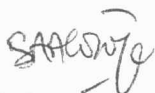
CIRCULAR ON THE NEED TO COMBAT CARD FRAUD

Following the increase in the spate of complaints by ATM cardholders on fraud, it has become necessary for all Deposit Money Banks (DMBs) to put measures in place, in addition to the existing guidelines to stem this tide. Consequently, all DMBs are hereby directed to implement the following:

1. No debit card should be issued on an account without a written request from the account holder. Henceforth, DMBs shall bear liability for any fraud perpetrated with the use of cards issued without written request from the account holder, and such card must be delivered in such a manner that the confidentiality of the information is not compromised.
2. DMBs should set and implement mandatory daily limits for ATM cash withdrawals. All other related transactions, including POS and Web purchases should be subject to stringent limits as agreed and documented between the DMBs and their customers. It is the responsibility of the DMBs to ensure that the agreements are documented and that such limits are embedded within the card so as to automatically initiate a trigger when limits are exceeded.
3. The use of 2nd level authentication for internet transactions is now mandatory for all payment cards. It is the responsibility of the Issuer to ensure that transactions emanating from its web merchants are properly scrutinized and operations are permitted only after 2nd level verification.

4. DMBs must send SMS alerts to the telephones/email addresses of cardholders whenever there is a debit transaction via payment card. Evidence of the dispatch of such messages would be required in cases of non-receipt of the alerts by account holders as a result of telephone network failures.
5. Cardholders should be provided with a facility to block their accounts immediately from their mobile phones whenever the SMS alert is received in respect of suspicious transactions so as to prevent further fraudulent transactions from being perpetrated.
6. All card issuing banks should deploy fraud monitoring tools that have the capability to monitor the normal spending trends of a card holder as well as automatically stop abnormal transactions that are perceived to be fraudulent. The block shall only be lifted by express instruction by the Card holder.
7. The use of temporary staff, i.e., Students on industrial attachment/vacation job, NYSC members and contract staff for card management and issuance/ distribution of PIN mailers should be stopped forthwith.

Appropriate sanctions will be imposed for non-compliance.



A.S. ATOLOYE
DIRECTOR, BANKING & PAYMENTS SYSTEM DEPARTMENT