UBA PayManager and EMS Application Form

A. CUSTOMER DETAILS

Company Name	
Address	
City/ State	
Phone Number	
Email	

Company Account Details

Account Name	Account Numbers	Account Type (Savings, Current, Domiciliary)

B. Setup details

Select desired Product: **PayManager** ☐   **Expense Management System (EMS)** ☐

- What PayManager module do you desire?   Direct Credit ☐   Direct Debit ☐

- What form of third level authentication security do you desire?
  System generated PIN ☐   Secure token device ☐

- Administrators' Full Name and email address_____
  ➢ Administrator functions:
    1. Users Setup   YES ___   NO ___
    2. Transaction report   YES ___   NO ___
    3. User Activity Reports   YES ___   NO ___

- Full name and email address of personnel that would approve administrator's setups and modifications _____

- File server address (Optional): _____

- Mandate Details

i. Batch transactions amount limit _____

ii. Individual transaction amount limit _____

iii. Do you desire transaction verification? YES ___ NO ___

iv. Would signatories approve transactions in piecemeal approval? YES ___ NO ___

- How many days should it be opened? _____

- Is Foreign Currency Payment desired (PayManager only)? YES ___ NO ___

- Would simplified data file be used for all uploads? YES ___ NO ___

  ➢ If YES, should third party code be system generated? YES ___ NO ___

- Would you also want to access this service at any UBA Branch? YES ___ NO ___

- Signatories

Full Name	Designation	Signatory Level	Account number and Approval limit (N)	Signature	Email address

Please attach passport photographs of all signatories with name and signature of each signatory on the flipside

* See glossary of terms on back page

Certification

I_____ hereby certify that the information provided above is correct and complete.

Full Name	Designation	Signature	Date

C. For Bank Use Only

	Account R. Manager	Branch Op. Manager	Branch Manager
Name			
Signature			
Date			
Email Address			

Glossary

Authentication code: this is a PIN that is sent to the final signatories email box before final transactions are sent for payment.

Approval limit: highest amount in Naira that a signatory can approve

Administrator functions: These are the roles that a client administrator can perform

Batch transaction amount limit: highest amount in Naira that a file of transactions should contain

Branch Usage: transactions can be processed by the bank branch on behalf of customer

Client ID: is used to identify the client accessing the system during logon

Direct Credit: funds transfer to a specified account

Direct Debit: funds transfer from specified account

Expense Management: Module for managing and funding UBA cashcards

Foreign Currency Payment: This is for making payments in currencies other than the Naira

File server address: This is the path where documents to be viewed by signatories resides

Group name: Name of group that a signatory belongs to. Example Manager Group, Director Group etc

Individual transaction limit: highest amount in Naira that payment to a single beneficiary can be

PayManager: Direct credit and direct debit system

Piecemeal approval: this allows for some transactions to be approved from a batch while the balance transactions can be treated later depended on the number of days set for it to be open

Secure token device: this is a hardware that generates a PIN every 60secs. It is to be used by final signatory before transactions are sent for payments

Signatories: approvers of payment transactions

Signatory Level: position of approvers (1st signatory, 2nd etc)

System Administrator: personnel that would manage system on client's behalf. This includes setting up users, downloading reports, assigning rights and privileges etc

Third party: this is a beneficiary or a remitter

Third party code: this is a unique code used to identify each third party on the system

Transaction report: records of transactions on the system can be viewed

Transaction verification: This ensures that a second level check on transactions uploaded is done and approved

Simplified data file: an upload file that contains a third party code, currency to be paid in and amount. For this to happen, all third parties would have been registered on the system with a corresponding third party code

System generated third party code: this is a unique code that is generated by the system to identify each third party. Code can also get manually generated by data entry staff

Users Setup: this is a function where an administrator sets up new personnel on the system and assigns them functions

User Activity Reports: logs of every action carried out on the system can be viewed using this function

PM SPECIFIC TERMS AND CONDITIONS GOVERNING UBA'S PAYMANAGER SOLUTION

1. SCOPE OF SERVICES\ FEATURES OF SOLUTION

1.1 Ability to effect instant debit of corporate account in UBA and credit on accounts in any bank on the Interswitch network;

1.2 Web based system which allows solution to be used from any location with internet access;

1.3 Workflow for multiple signatory approvals before final payment is consummated;

1.4 Module that allows for draft payment to beneficiaries;

1.5 Comprehensive reports on transactions;

1.6 Secure system that generates authentication code on the fly for final payment to be consummated;

1.7 Alert system to notify users of when transactions are pending for their action;

1.8 Libraries of transactions that can be stored and reused;

1.9 Ability to effect standing order transactions;

10.0 Card management system

10.1 Foreign currency payment capability

10.2 Direct Debit on third party's bank accounts in Nigeria and Credited to Corporate collection account real-time online

10.3 Simplified data file for data entry

10.4 Acceptance of User and system generated third party codes

10.5 A comprehensive Third party management module

2. USERS

2.1 The UBA PayManager Solution ("the Solution") is available to corporates maintaining Current and/or Savings account(s).

3. SECURITY SYSTEM

3.1 Unique access codes (Username and password) for each user;

3.2 Authentication code to finalize transactions;

3.3 Data is transmitted using 128 bit SSL certificate;

3.4 Data is stored in database encrypted;

3.5   Maker-checker mechanism for every action carried out on system;

3.6   Comprehensive activity logs;

3.6.1   PIN change to lock cards to organization

3.6.2   PIN change before first funding

4.   USE OF UBA PAYMANAGER SOLUTION PASSWORD

4.1   Each Customer shall be assigned a Password by the Bank, details of which must be kept secret by the Customer.

4.2   The Password will grant the Customer access to details about the Account, and the ability to authorize transactions in respect of the Account through the Solution.

4.3   The Customer must change its Password:

4.3.1   Immediately after first use of the Solution, to one formulated by it;

4.3.2   As often as possible after formulating it to reduce the risk of compromise to the Solution;

4.3.3   As soon as it suspects that its password has been disclosed;

4.4   The Password must not be disclosed or made known to any other person or entity including members of staff of the Bank by the Customer. If written, the Password must not be recognizable as a Password and must be kept separate from the Solution or any related documentation.

4.5   In the event that it is not possible to effect an immediate Password change when a Customer suspects that its Password has been compromised, the Customer must notify the Bank or suspend itself from use of the Solution:

4.5.1   By telephone or in writing immediately the Customer discovers the compromise of the security of the Solution; and also

4.5.2   Confirm in writing within 24 hours the compromise of the security of the Solution.

4.6   The Customer shall be liable for all transactions that take place up to 1 hour, within a Business Day, after the Bank receives notification that the security of the Solution has been compromised.

4.7   In the event that there are insufficient funds in the Account to pay for any Banking Transaction or other amount payable from the Account, including any interest, fees, charges or other payments due to the Bank, the Bank may in its own absolute discretion transfer sufficient funds from any other account maintained by the Customer with the Bank to the Account.

4.8   If the Customer deliberately, inadvertently or negligently discloses the Password to any person or entity, resulting in unauthorized transactions on the Account(s),

the Customer shall be solely liable for those transactions and the Bank shall not be liable for any losses incurred thereby by the Customer.

4.9   If a Customer forgets its Password at any time it will be required to advise the Bank in writing, through its branch, whereupon arrangements will be made to have the Password reset.

4.10   For security purposes and to maintain the highest level of service, there shall be an audit trail of transactions between the Customer and the Bank.

4.11   The Bank is hereby authorized by the Customer to act on all instructions received in respect of the Account(s), via the Solution, and to debit and credit the Account(s) with the amount of all transactions initiated via the Solution provided that, all instructions shall be authenticated by the use of:
(a)   the Password;
(b)   Any other procedures which may be agreed in writing between the Customer and the Bank.

5.   TRANSACTION LIMIT

5.1   In the case of the transfer of funds from the Customer's Account, the maximum sum which can be authorized in any one Day shall not exceed =N=………… (…………. naira) or such other sum as the Bank and the Customer may agree in writing.

5.2   Provision of the Solution will not entitle the Customer to overdraw the Account(s) if borrowing arrangements have not been made with the Bank nor to overdraw in excess of any borrowing limit agreed by the Bank.

6.   LIMITS OF LIABILITY AND INDEMNITY

6.1   The Customer shall be liable for all losses arising from the misuse of its Password with the Customer's consent or due to his negligence.

6.2   The Customer will not be responsible for any transactions if a Password is misused before it receives it but it shall be obliged to notify the Bank under clause 4.5 above.

6.3   The Bank shall not be responsible for any transaction failure under any circumstances including, but not limited to, the following circumstances:

6.3.1   Where there are insufficient funds in the Customer's Account at the time of the transaction;

6.3.2   where the Account has been temporarily or permanently suspended due to violation(s) of any of the provisions of these Terms and Conditions;

6.4   If a payment instruction is hijacked in transmission, this does not necessarily result in exposure on the part of either the Bank or the Customer as the transaction flow requires the content of the files to still be reviewed by other officers of the Customer either at the pre-payment stage or during the stages of final authorization.

6.5 In the event of identity impersonation, where a user has gained unauthorized access to the application, various controls have been built into the application to render this compromise ineffective. Some of these controls are:

6.5.1 Authentication code before final authorization
6.5.2 RSA secure token before final authorization

6.6 In the case of a total system hijack by an unauthorized party, which leads to damaging events to the Customer's account, the liability of the Bank will be a function of:

6.6.1 Clear proof that the breach is not as a result of negligence on the part of the Customer or any of its empowered officers. Such negligence include but is not be limited to related actions such as the misplacement of passwords and/or security tokens or evidence that the electronic instruction was facilitated by the use of the passwords and/or token of any of the officers of the Customer.

6.6.2 The Customer allowing UBA to conduct a periodic (quarterly) review and risk assessment of the related application resident in the Customer's environment.

7. FEES/CHARGES

7.1 The Customer hereby authorizes the Bank to debit the Customer's Account(s) the sum of N_____ (_____ only) commission per transaction.

7.2 Details of such charges are available on request from the Bank, and the Bank reserves the right to apply the relevant charges for any further services that may be introduced and utilized by the Customer.

8. GENERAL

8.1 The Solution must not be used:
After one or more of the security features on the Solution has been compromised;

8.2 Once the Solution has been used for a transaction, the transaction cannot be stopped or reversed.

8.3 The Customer must take all reasonable precautions to prevent unauthorized use of the Solution.

8.4 A direct debit mandate shall be obtained from Third party(s) before the account(s) is debited

8.5 Only cash-cards issued by the bank shall be used on the EMS

Sign off

I_____ acknowledge that we have read and understood the terms and conditions and security precautions stated therein.

Full Name	Designation	Signature	Date