NFIU/EXT/PUB/GUIDE/AC-STEI/JUL-2022/VOL.I/011

UPDATED OPERATIONAL ALERT ON EMERGING TREND OF MONEY LAUNDERING THROUGH AGENT BANKING: FOCUS ON POINT OF SALE (POS) BUSINESS

July 2022

INTRODUCTION

In October, 2020 the Nigerian Financial Intelligence Unit (NFIU) issued an operational alert on emerging trend of money laundering through Agent Banking with focus on Point of Sale (POS) business. This was at a time the COVID-19 pandemic caused disruptions to traditional banking operations.

The operational alert provided indicators for money laundering carried out through agent banking, specifically the use of POS terminals. Reporting entities were advised to leverage on the indicators provided in combination with other observable threats to identify potential money laundering activities via the operations of these agents.

As a result of physical restrictions, Nigerians conducted electronic transactions in just four payment categories (POS, E-Bills Pay, NIP and ACH) summing up to N178 trillion in 2020 alone, higher than the N119 trillion reported the year before[1].

Nigeria's National Risk Assessment (NRA) was updated in 2022 and involved the assessment of the inherent vulnerability of agency banking which was overall rated High; with its inherent characteristics, nature of product & service, nature of clients, geographic reach and nature of delivery all equally rated High. This vulnerability is further reinforced by reports that POS operators hanging around area commands and police stations formed part of a ring of extortionists operating at police formations thereby facilitating extortion of suspects by police officers[2].

To further provide guidance to competent authorities as well as reporting entities, the NFIU is updating the operational alert with case studies that demonstrate the use of POS in carrying out money laundering and terrorist financing. The vulnerabilities and corresponding mitigants have also be updated based on findings from the NRA.

Source: © restofworld.org

[1] https://www.premiumtimesng.com/business/business-news/486885-as-covid-shut-businesses-in-2020-only-four-nigerian-banks-made-more-money-online.html

[2] https://dailytrust.com/police-to-arrest-pos-operators-aiding-extortion-at-stations-in-lagos

BACKGROUND

AGENT BANKING

Agent Banking is a simple user friendly and cost-effective way of providing secured light banking services such as Cash deposit, Cash withdrawal, Fund transfer, Bills payment, Airtime Recharge, BVN etc. to people in a community, employing known and trusted existing retail business outlets in the same community. Authorized Bank Agents process these transactions quickly and easily via platforms such as Point-of– Sale (POS) terminals or Mobile Phones.

It is a cost-effective solution designed to provide financial access to the unbanked and underbanked population. The national financial inclusion strategy is aimed at reducing financial exclusion to 20% by the year 2020 and Agent Banking is part of the process to help achieve this target.

Agent banking began in 2013, after the Central Bank of Nigeria (CBN) released its guideline on the operations and management of the business. Since then, it has remained one of the retail channels of several commercial banks to make their banking services reach a large number of people.

There are two Agent Banking models in Nigeria: Bank-led where a financial institution acts as the principal; and Non-Bank led where a corporate body acts as the principal of Agent Banking.

The models operate in three categories - the Sole-Agent, Super-Agents and Sub-Agents in the network.

Agent Banking is also facilitated by Mobile Money Operators (MMOs). The Agent Banking relationship is commission-based.

Agent Banking networks are widely spread across the nation with limited integration with other sectors of the economy. They have no international reach and cannot transact in foreign currency.

As at 31st December 2021, Agent networks numbered 1,002,514 (one million, two thousand, five hundred and fourteen) exceeding an anticipated figure of 1,000,000 agents projected by the Central Bank of Nigeria[3], CBN at the end of 2021.

The agents conducted a total of

[3] CBN Agent Banking Report, 2021

1,040,301,601(1.04 billion) transactions in 2021 valued at **N17,495,388,763.00** (Seventeen billion, four hundred and ninety-five million, three hundred and eighty-eight thousand, seven hundred and sixty-three Naira) equivalent to 42.4m(USD). 88.7% of these transactions were cash deposits and withdrawals[4].

AGENCY BANKING SWOT

Strengths

- Lower cost than building traditional bank branches, hiring fixed employees
- Commission based costs supports scaling Agency network, variable financial case
- Helps lowers queues in bank halls
- Can support retailer/SME banking business line

Weaknesses

- Lack of real control of agent behaviour, cash control
- Requires a "partner management" programme/systems/people
- System or power failure
- People have trust issues
- Rural people are not techy

Opportunities

- Tendency to leave money in bank account, with easier access/more locations
- Combined behaviour (banking and agency location activity) can increase number of banking moments, joint activities
- support card usage (if using POS)
- can generate new bill payment revenues (incl. taxes, school fees) in some markets
- can increase customer base

Threats

- bank reputational risk if things go wrong
- fraud practices
- sources of funds

POINT OF SALE

A Point of Sale (POS) is a place where a customer executes the payment for goods or services and where sales taxes may become payable. A POS transaction may occur physically or online, with receipts generated either in print or electronically.

[4] 2022 NIRA Agency Banking Profile

AML/CFT VULNERABILITIES OBSERVED IN POS BUSINESS

Despite the advantages of POS business and obvious guidelines on their management, the sector is still susceptible to Money Laundering and Terrorism Financing.

The following are AML/CFT vulnerabilities inherent in POS transactions determined from previous research and risk assessment:

- **Cash-based**: Due to the cash-based economy a high proportion of POS transactions involve cash. Customers deposit and withdraw huge amounts of cash which makes the business vulnerable or attractive to money laundering.

  An agent can accept deposit into customers' bank account from any location in Nigeria. Though there are limits to such deposits but cash-in can be structured between an agent and the customer involved to suit an unusual circumstance that may not be easily acceptable by the bank. The Agent's account with the bank is used in this instant instead of the customer's account. This is very vulnerable to ML and TF.

  Agents also provide cash withdrawal services to bank customers using its network. This is particular with super agents that have their main network in the cities with numerous sub agents in other remote destination.

- **Money Laundering through use of unscrupulous Banking Agents**: Professional Money launderers can provide unscrupulous banking agents with huge illicit sums of money to move into the financial sector through series of transfers to different bank accounts. Furthermore, money mules can be used to easily transfer proceeds of crime to criminal organisations or terrorists.

- **Lack of proper identification mechanism and KYC**: There is little or no process/procedure to identify customers before performing transactions. This makes it possible for the customers to move illicit funds.

- **Lack of proper documentation of transactions**: Customers transaction details are not kept for future reference by regulators and law enforcement

agencies.

- **Easy to conduct**: Customers can easily get value in cash immediately the accounts of the Merchants are credited without knowing the source and destination of the funds.
- **Fraudsters can exploit the business**: Compromised banking details could be used by fraudsters to transfer funds from victim accounts to the POS merchant, then receive cash.

  There are cases of fraud reported[5] in relation to connivance between bank staff and POS operators. This will further heighten the vulnerability associated with the product/service
- **Compromised cards**: fraudsters can use stolen debit/credit cards and use them to carry out transactions at POS terminals.
- **Fraud by POS merchants**: some POS operators can overcharge customers on their commission by charging higher than the agreed amount. They can also carry out skimming fraud by stealing card details of customers to clone their cards which will be used to make unauthorized withdrawals from their accounts.
- **Fraud by Customers**: There could be network issues resulting to failure or reversal of transaction after the customer has received value and left the premises of the agent.
- **Armed Robbers exploit versions of POS Machine**: The android version of POS machine is the kind being used by armed robbers because it gives no details of the transactions carried out on it. This is because the SIM that is attached to the PoS account with which the agent receives bank alert for every transaction is different from the SIM that is used to operate the machine[6].

[5] https://www.premiumtimesng.com/news/more-news/473150-efcc-arraigns-four-for-n900-million-pos-fraud.html

[6] https://tribuneonlineng.com/report-robbers-fraudsters-using-pos-to-us-we-will-take-swift-and-appropriate-actions-lagos-police/

CASE STUDIES INVOLVING THE USE POS TO COMMIT CRIME

USE OF POS OPERATORS TO TRANSFER FUNDS FOR TF

A Financial Institution X filed a Suspicious Transaction Report (STR) to the Nigerian Financial Intelligence Unit (NFIU) on its customer A for possible terrorist financing.

Customer A is a 31-year-old male, residing in Zauda Village Abuja. He is known to be a **POS operator** and has made several huge cash deposits as well as significant transfers from his linked Z Bank account. He operates in an area that has no banking hall and therefore usually collect money from numerous people and deposit same at the nearest banking institutions which are located in **Kubwa and Dei-Dei-Abuja.** Customer A's account has been in receipt of cash/transfers totalling **₦1,601,635,500.00** (One billion, six hundred and one million, six hundred and thirty-five thousand, five hundred naira in **237** (Two hundred and thirty-seven) count transactions deposits between the period of 2021. These amounts where received from different unknown depositors. Most of the deposits were done by the subject in his bank account using cash which are then disbursed to other individuals with transaction descriptions used to identify the depositors, some of the narratives were given as **Alkaida** and **Gun,** indicating a possible link to extremism.
The NFIU analysed the STR and disseminated the intelligence report to a LEA for further investigation.

Terrorist Financing Feature of the STR:
The large cash inflows and quick transfers with the suspicious narratives **Alkaida** and **Gun.**
Abuse of POS anonymity by suspected terrorists to move funds to their associates as no means of identification is required to consummate transactions

USE OF POS TO MOVE PROCEEDS OF KIDNAPPING FOR RANSOM (KFR)

A Financial Institution X filed a Suspicious Transaction Report (STR) to the Nigerian Financial Intelligence Unit (NFIU) on its customer A for possible Kidnap for ransom.

Customer A is a farmer residing in Kaduna. Customer A has been identified by the FIU analysis to be linked to kidnappers, was seen to have used POS merchants to move about 10 million naira in one month in the year 2021.

In the month of March, 2021, Customer A withdrew a total of N10,849,000.00 (ten million, eight hundred and forty-nine thousand naira only) via POS merchants in and around **Kaduna**. On 3 occasions, single POS withdrawals ranged from N1million to N2.7million within the same period, he has received funds transfers of about N9million from different individuals. These transactions coincided with increase in Kidnap for Ransom incidences in Kaduna State.

One of these POS operators is Mr. C who is a 26-year-old Nigerian residing in Kaduna State is linked to multiple accounts used for POS operations within the same region.

Within a period of one year beginning from September, 2020, two bank accounts operated by Mr. C received inflows totalling N400 million. In one of the bank accounts maintained by Mr. C, received cash deposits within a period of 5 months in 2021 totalling N109 million.

There was consistent mopping up of funds from one of the bank accounts of Mr. C into the bank account of Customer A. This transaction pattern occurred from the beginning of 2020 to August, 2021. Transfers to Customer A from Mr. C in the month of March, 2021 totalled N10million.

The FIU analysed the STR and disseminated the intelligence report to a LEA for further investigation.

USE OF POS OPERATORS TO FACILITATE FRAUD

A Financial Institution X filed a Suspicious Transaction Report (STR) to the Nigerian Financial Intelligence Unit (NFIU) on its customer A for possible fraud.

Customer A is a 22-year-old male residing in Abuja, Customer A opened his account with the bank on **25th March 2020**. Customer A fraudulently received multiple unauthorized funds via mobile transfer of N3,499,000.00 (three million four hundred ninety-nine thousand naira only) from Mr. B whose account is domiciled in a different bank.

Mr B is a lecturer in a University in Kwara State. The reported transaction was done possibly through swapping of the mobile number linked to Mr. B personal account as there is no established relation between customer A and the Mr. B. The Customer is possibly in a crime syndicate, where he and his partners hack into unsuspecting victim's internet banking profile and thereby divert funds to accounts where they have interests.

A review of the transaction history showed that the reported transaction is the only significant transaction on customer A account since inception in 2020. Furthermore, when the funds were fraudulently received into customer A's account, he immediately made multiple POS withdrawals at different POS vendors. Customer A abandoned the account after all withdrawals were done.

The NFIU has provided intelligence to the Nigerian Police Force for further investigation.

USE OF POS TO AID BANDITRY

A Request was made on Mr. A by a Law enforcement agency, Mr A was being investigated for possibly aiding payment of logistics for bandits in Nigeria.

Mr. A is a 49-year-old Nigerian residing in Kaduna State, which has been plagued by multiple bandit attacks. Mr A. was not seen to have any known source of income.

Furthermore, Mr. A was seen to have received huge inflows and outflows between 2020 and 2022. Prior to these huge transactions Mr. A was transacting in bits from 2015 to 2019.

In the year 2022 the Mr. A was seen to have received N7,676,920.00 (seven million six hundred and seventy-six thousand nine hundred and twenty naira only) from multiple POS vendors in multiple transactions. These POS vendors include **POS Agent AA**, **POS Agent JG, POS Agent N,**

POS Agent A and **POS Agent MS**. The purpose of this transactions was not verified and the transaction showed a sharp shift from Mr. A pattern of transaction, which seems a bit.

The FIU has furnished the LEA with relevant intelligence to aid their investigation.

USE OF POS TO FACILITATE RACKETEERING, CRIMINAL CONSPIRACY AND FRAUD

Mr. X, a male furniture maker residing in a town in Nassarawa State was investigated by a law enforcement agency (LEA) in respect of racketeering, criminal conspiracy and fraud. He is reported to own nine (9) bank accounts.

Analysis of one of Mr. X's accounts revealed that within a month in 2021, there was a total deposit of **₦3,722,699.04** (Three million, seven hundred and twenty-two thousand, six hundred- and ninety-nine-naira, four kobo). Mr. X made a total withdrawal of **₦3,724,342.39** (Three million, seven hundred and twenty-four thousand, three hundred- and forty-two-naira, thirty-nine kobo). Transaction dynamics on the account show cash withdrawals via POS by Mr. X on the same day he receives any bulk or a large sum of money at two (2) specific **POS VENDOR 1 LTD** and **POS VENDOR 2 LTD**. These POS vendors are both Nigerian companies registered with the Corporate Affairs Commission (CAC).

It was recorded that Mr. X's account received five (5) transactions totaling the sum of **₦1,139,814.04** (One million, one hundred and thirty-nine thousand, eight hundred- and fourteen-naira, four kobo) from one Mr. L between 1st July 2021 and 22nd July 2021. It was revealed from transaction analysis that Mr. X was being paid for services such as Visa Work permit family and Labour Market Impact Assessment (LMIA) fees. These are similar or comparable to a foreign country recruiter or labour-hire fees or is planning to relocate to a foreign country. It was also discovered that on July 2021, **₦962,135.00** (Nine hundred and sixty-two thousand, one hundred and thirty-five naira) was transferred into this account as payment for flight tickets. Between 14th July, 2021 and 22nd July, 2021, the subject further received a total of **₦1,505,000.00** (One million, five hundred and five thousand naira) into this account in seven (7) transactions from unconfirmed sources. Mr. X then made total withdrawals of **₦2,823,000.00** (Two million. eight hundred and twenty-three-four thousand naira) through **POS Purchases** in thirty-seven (37) transactions from this account from **POS VENDOR 1 LTD** between 1st July, 2021 and 22nd July, 2021, while on 23rd July, 2021, a sum of **₦388,000.00** (Three

hundred and eighty-eight thousand naira) was withdrawn by cash from his account through **POS VENDOR 2 LTD.**

USE OF POS TO FACILITATE FRAUD AND EXTORTION

The transactions of Mr. DX were flagged as unusual and reported to the NFIU. Between 3rd September 2020 and 11th September 2020 Mr. DX's account received inflows totalling N1,200,000.00 (one million two hundred thousand naira only) from multiple senders largely via POS and USSD from three individuals; T, B and P. a majority of the inflows, constituting 96% of the total was received on 3rd September 2020.

Upon receipt of the funds Mr. DX made various ATM cash withdrawals and some account transfers to few other individuals.

Based on the pattern of transaction observed on the subject's account, the NFIU is inclined to believe that the subject is likely involved in fraud or extortion. An intelligence report was sent to law enforcement agency for investigation.

ML/TF INDICATORS THROUGH THE USE OF POS TERMINALS

- A POS operator should scrutinize transactions with the following elements;
- A remote POS terminal suddenly carries out large consistent transactions in batches of small and large sums.
- Multiple deposits and withdrawals from same account on the same day, without charging or receiving a commission.
- Deposits made into accounts of POS operators with narrations related to extremism, terrorist groups or instruments of terrorism.
- Customer carries out transactions in large sums which may not be consistent with his known source of income.
- Customer receives/sends funds transfer from/to areas of armed conflict/prone to Terrorism/TF/high risk jurisdictions and transfer such to one or different individuals immediately
- Customer frequently transfers funds from various accounts to the POS merchant and always withdraws in cash.
- Customer who appears to rush the POS merchant in receiving cash before the receipt is printed under the guise of being in a hurry.
- Receives wire transfers in batches below the threshold from different individuals or companies to avoid reporting.
- POS agent is linked to multiple accounts used for POS operations within the same region.
- Customer carries out transactions with multiple cards that have different names or owners.
- Customer makes multiple withdrawals at the different POS outlets on the same day to truncate audit trail.
- Customer unwilling to present identification to support the name on card.
- Customer inputs different wrong PINs for payment cards without success.
- Customer receives sudden inflow of large electronic transfer and cash

deposits; followed by an increased outflow immediately after transaction.

- The abuse of POS anonymity by suspected bandits who use these POS merchants to move funds.

CONCLUSION

It is imperative to strengthen and support Government's strategy on financial inclusion, compliance to the rules and regulations on the management of Agent Banking so as to prevent money laundering, terrorism financing and other predicate crimes that may be perpetrated by fraudsters due to the vulnerable nature of the business.

THOUGHTS ON POSSIBLE SOLUTIONS

Based on our assessment of POS business operations in Nigeria, it is believed that absence of strong due diligence portends that criminals will be able to wash their illicit funds or move same for criminal purposes with ease. There is therefore an urgent need for regulators to be broad and deep improvements to financial crime supervision and encourage knowledge, resources and technologies needed to prevent the everchanging criminal networks from exploiting the status quo. The operational alert further recommends the following:

Role of Regulators: Competent authorities saddled with inspection responsibilities should ensure compliance on;

- All guidelines and regulations by the CBN and other sector regulators on Agent banking
- Guidelines on adequate record keeping of transactions
- Implore latest transaction monitoring systems for detecting anomalous transactions in line with international best practice.
- Conduct meticulous KYC on Banking Agents and only grant license to people of integrity to avoid abuse of the system
- Regulator to ensure Banks/MMOs comply with their obligations to monitor agent's activities.

Role of Banking Agents/POS operators: the operators should ensure the following:

- Routinely train POS operators on the concept of AML/CFT.
- Identify Red flags and indicators of ML/TF through the POS machine.
- Keep proper records of transactions.
- Conduct KYC on customers.
- Procedure for reporting suspicious activities of suspicious customers.
- Report suspicious activities through relevant channels.
- Keep proper records of all transactions.
- Liaise with banks to acquire electronic record tracking devices such as the biometric authentication machine that would help verify customers in line with KYC principles.
- Learn the procedure for reporting suspicious activities of customers.
- Report suspicious activities through relevant channels.
- Maintain integrity and professional ethics in the course of their work.
- Continuous review of products and services with the risks associated.

'Professional Money launderers can provide unscrupulous banking agents with huge illicit sums of money to help get the money back into the financial sector through series of transfers to different bank accounts.'