Unizik Journal of Business
www.ubsjournal.com.ng
Volume 4(2), 2021
DOI: 10.36108/unizikjb/1202.40.0270

EVALUATING GOVERNANCE PRACTICES AND BUSINESS OPERATIONS IN NIGERIA: ATTENDANT RESPONSE TO FRAUD PREVENTION AND RISK MANAGEMENT IN THE COVID-19 PANDEMIC ERA

Emma I. Okoye, PhD

Professor of Accountancy and Director of UNIZIK Business School, Nnamdi Azikiwe University, PMB 5025, Awka, Anambra State, Nigeria

&

Ugochukwu J. Nwoye, PhD

Department of Accountancy, Nnamdi Azikiwe University, PMB 5025, Awka, Anambra State, Nigeria.

ABSTRACT:

Despite the outcome of the COVID-19 pandemic onslaught on global economies that has negatively undermined the financial prowess of major markets in United States of America, United Kingdom, Germany, France, Austria, Canada, Spain, Italy, Nigeria, South Africa, Ghana et cetera, leading to loss of trillions of US Dollars, the need to uphold responsive financial sustainability among nations and businesses has been largely impaired by the prevalence of fraud, cyber crimes, mismanagement of scarce finance resources and external loan funds, bad leadership and poor oversight. Amid unprecedented increase in job layoffs, salary cuts, expenses cuts, robotic technologies embrace, bonuses suspension, promotions postponements, remote working embrace, price hikes, high inflation rate et cetera which have all culminated into heightened fraud occurrences and consequent fraud losses, fraud risk appear not to be proactively considered a top priority by the government and management of businesses in critical challenging COVID-19 pandemic economic downturn period as this. Deploying a descriptive approach, the study expressly evaluates the threat of COVID-19 pandemic upsurge on public governance and businesses with extant emphasis laid literally on attendant responses to fraud prevention and fraud risk management in Nigeria. Conceptualized schematic frameworks and widely recognized current statistics were utilised and evaluated to maximally envisage reliable response measures to fraud risk factors in the contemporary COVID-19 pandemic business environment in Nigeria. The study concludes by proposing possible actions (way forward) for policies development towards rescuing Nigeria and its business environment from the prevailing unfavourable situations.

Keywords: Businesses, COVID-19 Pandemic era, External loan funds, Fraud, Fraud Risks, Financial resources mismanagement, public governance.

INTRODUCTION

With the upsurge of the Coronavirus Disease pandemic in 2019, otherwise known as COVID-19 pandemic globally in February 2020, the International Capital Market was thrown into imminent chaos as many big businesses headed for the rock. The pandemic forced the financial markets to quit different trading fronts with enormous consequence on the world economy. The outcome was the outburst of COVID-19 related job losses across the globe; Nigeria being a typical example. Aside Stock Markets in China that remained generally strong and afloat, financial markets in United States of America, United Kingdom,

Germany, France, Spain, Italy, Nigeria, South Africa, Ghana et cetera, were gravely hit. The situation in several other African Capital Markets was rather a sorry sight with share prices trend dropping significantly and continuously. The implication was that Trillions of US Dollars worth of bond yields, oil revenue, and equity prices were lost globally within months of the pandemic outbreak in February 2020.

Developing nations like Nigeria, Ghana, South Africa, Congo DR et cetera took to policies response measures by easing existing monetary policies, making impromptu higher allocation of government spending on health services while providing other notable economic stimulus such as reduction in fuel prices, grant of holidays on electricity bill payment, water bill payment, rent payment (in some African countries) et cetera. It is quite unfortunate that most of these unique palliatives were poorly managed, as was the case in Nigeria, through fraudulent means.

The achievement of commendable financial sustainability in any nation, among corporate organisations and businesses has been largely impaired by prevalence of bad oversight leadership style in place in several businesses across the globe. Suffice it to say that the problem with many developing countries, Nigeria a typical example, is not entirely non-availability of finance for businesses or scarcity of funds; it is the mismanagement of such monies, budget and loan funds as well as bad governance.

Indeed, fraud has metamorphosed from act committed by mere fraudsters or temporary staff of organizations to unethical conduct perpetrated by organized crime and fraud rings that deploy sophisticated means to override established basic controls enshrined in organisations in order to commit fraud. Globally, the United States of America is the most fraud-prone country with 34% of consumers likely victims of fraud. United Kingdom follows next with 33%, Canada is 29%, Germany recorded 27%, and Austria stood at 21% (FinanceOnline, 2021). ICAEW (2021) reports that fraud now costs businesses and individuals in United Kingdom about £137bn annually, with average losses now 8.58%, - an 88% increase since 2007. The scale of financial crimes is enormous with global estimates ranging from US$1.4 trillion to US$3.5 trillion annually (Ewa, Adesola & Eseneyen, 2020).

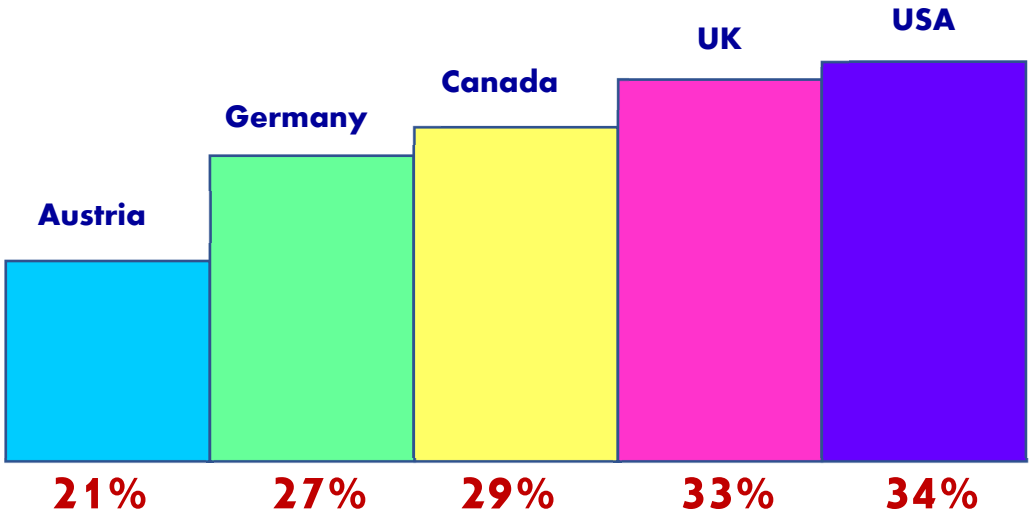

Figure 1: Most fraud-prone countries
Source: Authors' construct

Ibekwe (2012) reports that a second Africa Fraud Barometer result of KPMG, a global audit and financial advisory firm, portrayed Nigeria as having the highest number of fraud cases in both private and public sector on the continent of Africa. The cost of these fraud during in 2012 was put at N225 billion (US$1.5 billion). In 2017 alone, frauds and forgeries in the banking sector, according to a Nigerian Deposit Insurance Corporation (NDIC) report, amounted to ₦12.01 billion. A nation where the leadership swaddles borrowed funds for personal gain and selfish motives is certainly fraud driven and corruption endermic in nature. In the public sector, the citizenry expect accountability report as obtainable in the corporate/business sector annually in order to assess the performance prowess of those entrusted with the public sector resources. However, the reality of the situation on ground is so unfortunate such that the Law Makers, who are supposed to demand for accountability from the public officers, are corrupt if not more.

Despite the existence of Budget Monitory Price Intelligence Unit (BMPIU), the issue of inflated contract value or fees and consequent abandonment of non-executed contracts has continued to deteriorate unabated in Nigeria. A recent typical example is the shocking exposition of the shameful fraudulent activities at the Niger Delta Development Commission (NDDC) in 2020 running into billions of US Dollars, but this appears to have been swept under the carpet uninvestigated. At the moment, Nigeria's Due Process framework is a big fraud and scam that requires urgent rescue by professional Fraud Managers.

The Nigerian military is equally not left out as the US$1 billion foreign loan secured in 2015/2016 for procurement of new modern state of the art Arms and Ammunitions in the nations fight against terrorism is yet to be accounted for to-date. Soldiers have since died in their hundreds due to lack of Arms. Younger military Officers have continued to complain about the insensitivity of the federal government to their plight and welfare despite huge funds budgeted annually for this purpose. A situation whereby a Senator earns over N29 million monthly as wage in the same economic backward nation where fellow citizens are subjected to less than minimum wage of N18,000 (*the new N30,000 minimum wage is currently a paper-based pronouncement whose implementation is still far from reality*) that cannot purchase half a bag of local rice, is fraudulent and a direct reflection of no accountability in governmental practices.

Many studies suggest that fraud is more likely to occur when someone has an incentive (pressure) to commit fraud, weak controls or oversight provide an opportunity for the person to commit fraud, and the person can rationalize the fraudulent behaviour (attitude). The obvious truth is that the main driver of fraud is the innate desire for personal benefits or gains.

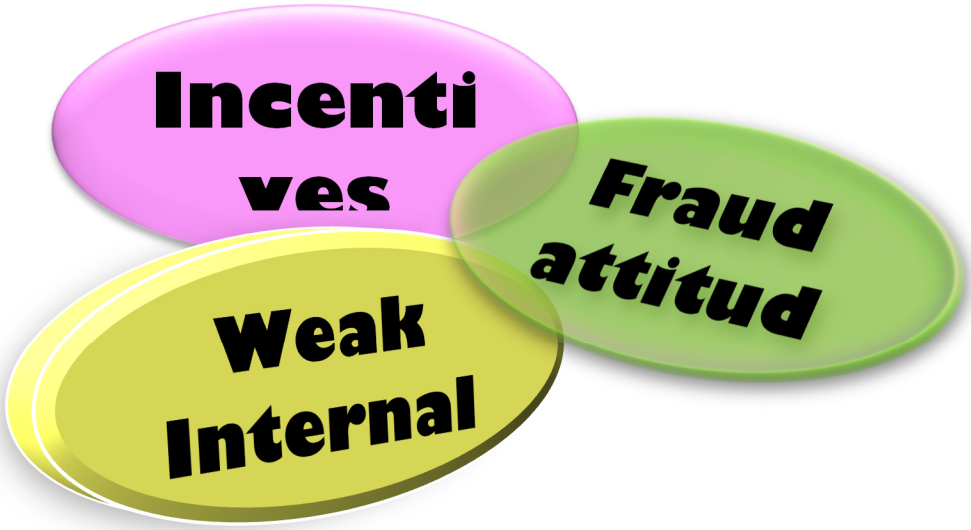

Figure 2: why fraud persist
Source: Authors' construct

Osisioma (2012) threw more alarming insight on this stressing that fraud is an industry complete with Stakeholders, Investors and risk-return profile. The fraud industry is organized, with internal coordination, shared knowledge and a vertical exchange of benefits linking principals and agents. It closes off clients' alternatives, creates a network of operatives, freezes out critics and non-corrupt Agents, and shares rewards and risks among stakeholders. The fraud system grows Practitioners at every level- from school entry stage to graduation, from childhood to adulthood, from micro to macro levels et cetera. There is a sustained supply of individuals and mean fellows who ensure that the system of fraud is maintained in perpetuity.

In view of these, this paper intends to:

1. Scholarly evaluate the threat of COVID-19 pandemic upsurge on the response of public governance and businesses to fraud prevention and fraud risk management in Nigeria.
2. Propose possible actions for reliable policies development purposes (way forward) towards rescuing the prevailing situation in the Nigeria.

MANAGING FRAUD AND FRAUD RISK

Contemporary Risk Management Approaches in COVID-19 pandemic era

Despite huge sum of money being recorded annually as fraud losses coupled with financial and reputational implications stemming from such fraud losses, Luis (2020) noted that fraud risk may not be considered a top priority by Management of businesses in critical challenging COVID-19 pandemic economic downturn as this. While most organizations may have resorted to cutting expenses, laying off employees, embracing robotic technologies, and encouraging employees to work remotely, the combination of these adverse conditions on employees' psyche appear to weaken employees morale, thereby heightening the risk of corporate fraud.

The danger of not understanding a risk and consequent mismanagement of such risk is not without its far reaching consequences, and should shed brighter light into this discourse. A look at the Nigeria public sector, for instance, revealed that the federal government spent 98% of its revenue on debt servicing between January and May 2021. This is considered a risky risk for a nation already gravely facing economic hardship amid

deteriorating state of insecurity, and that is quite worrisome. The above statistics is up from the 83% incurred by the Executive on behalf of the country in year 2020. This is more as the government had projected to spend N17.8 trillion on servicing debt between 2021 and 2024. Given the skeletal outlook of these indicators, it is Insightful to agree with Adebowale (2021) who noted that the federal government of Nigeria is actually in a mess with debt servicing. According to him, the federal government recently admitted spending N1.8 trillion on debt servicing from its N1.84 trillion revenues in the first five months of 2021 (January - May). This puts the federal government's debt-to-revenue ratio (a key measure of debt sustainability) at 97.8% for that period. Recall that the federal government's debt service to revenue in 2016 was only 44.6%. By year 2020, debt service-to-revenue had grown to 84.8%. These are far cry from the World Bank's suggested 22.5% for low-income countries like Nigeria. Does this not appear scandalous?

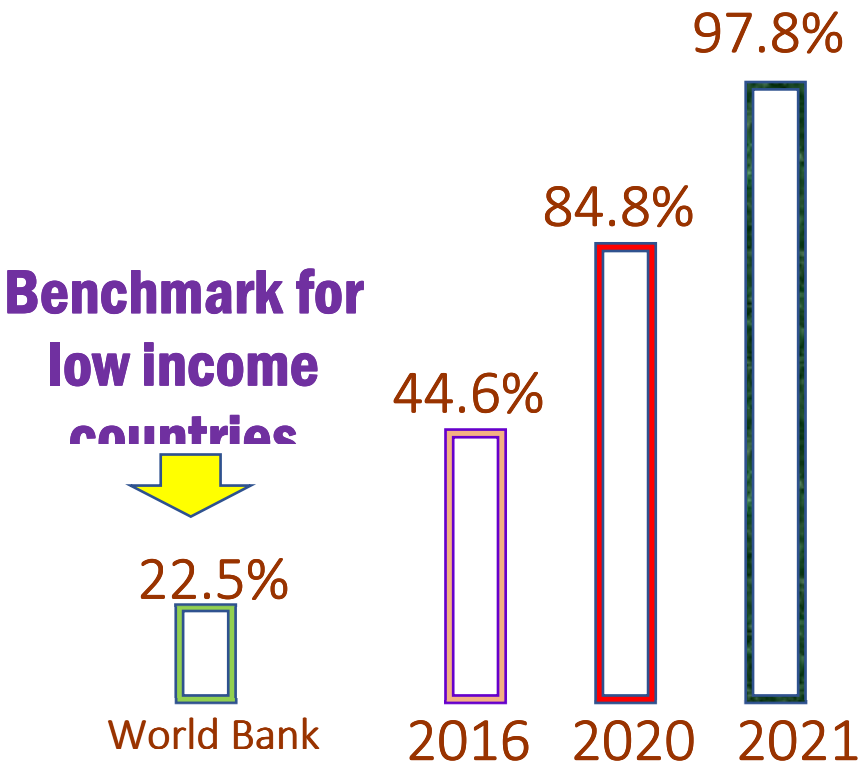

Figure 3: Nigeria federal government's debt-to-revenue ratio
Source: Authors' compilation

Amid these, the federal government through the President has officially reached out to the Senate on September 14th, 2021 stating its intention to picked yet another debt amounting to US$4.054 billion to bring Nigeria's foreign debt stock to US$45 billion. It is important to note that with this development, the total approved foreign borrowings in year 2021 alone totaled US$12.3 billion. With this, the country's external loan stock will have risen by 366% since year 2015, making debt servicing a serious burden to Nigeria and Nigerians. No nation can attain and sustain development with this kind of humongous debt settlements. This ugly scene is equally the present fate of some businesses in developing countries where annual business

revenue are exhausted in servicing loan obtained from banks for purported corporate investments.

However, it is pertinent to ask: of what economic benefits are these external debts to the country, its industries and the economy? How has the utilization of these borrowings benefited the Nigeria business environment over the years? How is the productive capacity of previous loans being measured? Which Arm of the Nigerian government weighs the possible risks involved? Are there high tendencies of fund mismanagement? Are these unethical practices vigorously being investigated? If yes, who conducts this investigation? Does it mean that Internal Audit Departments no longer exist in organisations, MDAs, parastatals, and ministries? If no, then who conducts internal audit on governments financial activities yearly? If yes, what do they do annually as Internal Auditors? How many of these Internal Auditors are well informed and independent professional Accountants?

Except these are objectively cleared, the risk of fraud will remain high and stares on sternly in Nigeria.

Perception of Fraud in Organisations

Fraud as an intentional deception made for personal gain in order to obtain unauthorized benefits such as money, property et cetera, can occur in government, non government and corporate organisations, in the form of *assets misappropriations, fraudulent financial reporting and corporate/business fraud.* This is more as all types of fraudulent activities are believed to fall under these three (3) major forms of fraudulent practices.

Asset Misappropriation schemes: With more employees working from home, oversight of employee behaviour may become more challenging. Some employees could face financial struggles providing them with certain incentives to misappropriate business assets for personal benefit (Thorps & Harding, 2020). Deloitte (2020) noted that existing internal controls could be more easily circumvented due to employees working remotely. The "*lets do this first and worry about the documentation and procedures afterwards*" attitude increases the risk of asset misappropriation and CEO fraud type of scams.

This type of fraud, in the COVID-19 pandemic regime, also include *theft of company's Assets* which in most cases take the form of inventory theft and fraudulent disbursement in the guise of overcoming the imminent demands of COVID-19 pandemic on work pressure, as well as *the misuse of company Assets* such as using a company's car or any other Non-Current and Current Assets for personal purposes.

Cash Theft: Of various mediums of Asset misappropriation, cash theft is considered the one less common in organisations in the COVID-19 pandemic era across the globe. Fraudulent tactics such as understatement and/or overstatement of financial activities in an organization are usually embraced by employees of organisations towards enriching themselves or making the organization appear so big to attract the investing public. Employ of schemes such as *'skimming'* which is the theft of off-book funds by understating turnover or revenue, omitting certain sales records, theft or diversion of incoming cheques to personal bank accounts et cetera. and *'cash larceny'* which is the opposite of skimming as it involves the theft of money that has already appeared on a victim company's books, are key channels through which cash theft is perpetrated in entities. A few other notable examples of cash larceny include unauthorized reduction in the unit price of purchases made by a customer, undue upward manipulation of the quantity or units of goods sold to deceitfully write-off fictitious inventories that were fraudulently held (*though not physically existent in the warehouse*) in the Inventory account of the company et cetera.

***Fraudulent disbursements*:** This is another on-book fraud scheme that explains how cash (cheques/transfers) fraudulently exits the savings and/or bank account(s) of an entity. This kind of fraudulent scheme is often recorded on the books of the entity, thereby leaving room for audit trail. Fraudulent disbursement schemes can be viewed from the following perspectives such as:

i. Cheques tampering schemes
ii. Register disbursement schemes
iii. Billing schemes
iv. Expense reimbursement schemes
v. Payroll schemes

***Inventory and warehousing fraud*:** This, on the other hand, involves undue misappropriation of an entity's inventory for one's personal use, theft of such inventory and scrap, or charging of cash embezzled to inventory to make it look as though the value of the fund embezzled is still in the company as account receivables (trade debtors) or inventory stored up in the stores/warehouses. Accordingly, accounts receivable, as a Current Asset item, is also very vulnerable to fraud. It is considered a major enabler of Financial Statement fraud schemes and Asset misappropriation schemes. Accounts receivable fraud can come in the form of Lapping (*diverting customer A's payment for personal use but records customer B's payment to customer A and customer C's payment to customer B*), Fictitious receivables (*set up in disguise as fictitious sales which is eventually written off at a latter period in the future*), and improper posting of credits (*posting a customer's credit payment in form of a discount, returns, or money written-off from customer's account all in effort to cover up a cash theft*).

Fraudulent Financial Reporting: The economic impact of COVID-19 may have created incentives and opportunities for companies to record fictitious revenue. Management estimates such as goodwill valuation are also at risk of misstatement. Accordingly, fraudulent financial reporting is the second major type of fraud that is deliberate and often committed by the *'management'* of *business or non business* organizations. This type of fraud usually injures the organisation's Investors, Creditors and other relevant Stakeholders through misleading Financial Statements. In other words, it is a scheme designed to deceive another or a third party whose interest in or reliance on the financial information or disclosures of the organisation is not in doubt. This means that the end goal of fraudulent financial reporting schemes is earnings management.

There is every need for professional Fraud Managers to have a firm grasp of minimum disclosures requirements expected of public listed or private owned corporate organisations to present during Financial Statement preparation. As a result, great care must be exercised to ensure that Financial Statements prepared and presented are duly compliant with approved and/or authorized accounting Standards applicable in the reporting jurisdiction of the corporate organsation. Globally, the International Financial Reporting Standards (IFRS) issued by the International Accounting Standard Board (IASB) from April 2001 is presently in use and mostly authorized by different reporting jurisdictions as the mandatory financial reporting framework for all public listed entities in all sectors. Small and Medium Scale Enterprises are also required to ensure full compliance with IFRS for SMEs disclosure guidelines in the preparation of Financial Statements in Nigeria. Studies have shown that the response of public listed entities in Nigeria to the implementation of IFRS is impressive. It is in the light of this that attention should be given to the operations of corporate entities as they intensify effort yearly to remain compliant to IFRS disclosure requirements in the COVID-19 pandemic era. This will also avail Fraud Managers the opportunity to thrive towards ascertaining whether quality assurance has been upheld by such entities and her employees within the corporate environment and its accompanying practices.

Some notable fraudulent financial reporting practices in the COVID-19 pandemic era are:

1. Recognition of revenue before sales is made.
2. Improper timing of revenue to meet revenue projection or target.
3. Much higher revenues than expenses.
4. Mismatch between tremendous growth in inventory and sales as sales made without

accompanying purchases, ordinarily lead to reduction in inventory.

5. Capitalizating expenses and cost against established/known industry norms and falsely attributing the same to long term COVID-19 response initiatives.
6. Deferring expenses from loss years to a future profitable year.
7. Entity reports growing earnings though cash flow continues to decrease.
8. Much higher growth in revenues than expected is recognised compared to that obtainable by other competitive companies in the same market and industry.
9. Unusual increase in book values of Assets.
10. Real nature of transaction disclosed is quite impossible to determine and understand.
11. Entity modified or deleted invoices in the manual or e-financial books.
12. Loans are written off to related parties.
13. Unexplained changes in uncollectible/non performing loan accounts.
14. Credit sale to customer's account was followed by immediate identical debit in entity's cash account.
15. Changes in entity's sales/turnover (increase or decrease) that is not consistent with changes in cash receipts.
16. Increase in credit level is not consistent with total sales recorded.
17. Inabilty to locate disclosures made in respect of cheques claimed to have been bounced or cancelled.

Corporate fraud: This is usually viewed as the third type of fraud that entities perpetrate. It is a type of fraud most featured and feared by business communities, as its occurrence is believed to have far reaching consequences on both internal and external parties. Regrettably, prevalence of corporate fraud often result in an inevitable loss of existing confidence previously reposed on the organization, the concerned capital market and the accounting profession and its professional practices. It is however worthy to note that the discourse of corporate fraud equally encompasses issues raised under asset misappropriations, fraudulent financial reporting and other fraudulent activities obtainable within an entity. Thus, this type of fraud cannot be discussed in isolation, implying that other areas already enumerated above must be considered as well for acceptable level of understanding of corporate fraud mechanism in the COVID-19 pandemic era to be attained. A few corporate fraudulent practices in the COVID-19 pandemic era are:

1. Unusual and unauthorized changes to customers' accounts.
2. New customer's account activated with unusual names/addresses.
3. Payment made or expenses incurred on entity's behalf are not properly authorized or clearly indicates that typical controls in the entity are overridden.
4. Unusual number of reversed transactions.
5. Unusual number of pricing alterations or overrides
6. Unusual number of credit sales overrides
7. Non-reconciled timing difference between cash collection period or claimed bank deposits and the time or day of posting such cash collections to entity's accounts.
8. Unauthorized payments for goods and services at a higher price than obtainable in the competitive market.
9. Unusual increase in cash collection period for credit sales or trade receivables collection period.
10. Observed different amounts paid to suppliers in respect of the same quantity of inventories supplied to the entity amid stable price during the period..

11. Management team maintains extra ordinary close relationship with customers or suppliers.
12. Certain Suppliers are not settled timely or being paid earlier than other suppliers.
13. Records reveal that one payment applies discount while another makes full invoice payment for the same inventory and quantity sold at the same price.
14. Credit limits allowable to customers exceeded without top management's approval.
15. Excessive consulting fees paid above feasible charges obtainable among other competent professionals for the same services rendered.
16. Employee exhibits a domineering/controlling attitude.
17. Employee displays controllable or uncontrollable strong desire for personal gain, even at the expense of the entity.
18. Often has a "too good to be true" work performance trend.

Why the rage of Fraud deteriorates in the COVID-19 pandemic phase

It is widely believed that people do not just wake up one morning and commit fraud. Certain persuasive factors must be responsible for such unethical actions and despite the accruing consequence of doing so. This is more as many organisations' fraud prevention strategies are no longer fit and effective to deter fraudulent activities in the COVID-19 pandemic era. ICAEW (2021) notes with regret that too many organisations are reactive-oriented to fraud, envisaging response to fraud only when losses have occurred. And despite fraud being an ongoing cost that makes businesses less profitable every moment it breathes and thrives, the idea of adopting proactive response measures is more pronounced than practiced among enterprises in Nigeria. Below is a few outline:

a. High rate of job loss/lay offs by corporate organisations in the COVID-19 pandemic period compels employees to store up something for themselves ahead of predictable hard times.
b. Need to remain in business in the face of emerging stiff government reforms and policies and deteriorating capital market performances remains a motivator responsible for concealment of losses or poor performance among businesses and public enterprises.
c. Resolve to meet periodical targets at all cost in order to secure periodical bonuses tied to performance.
d. Absence of robust internal controls is an express access door.
e. Poor oversight on entities internal controls is a major weakness that allow for greater exploitation of the entity by fraudulent employees and fraudsters
f. Pressure to maintain big face in the competitive market towards meeting external expectations of stakeholders and dividend earners remains a driving force.
g. The need to show steady income stream to impress investors and keep the share prices afloat in the Capital Market compel companies to engage in income smoothing.
h. Selfish desires for tax benefits especially where taxable income is measured through accounting numbers makes companies to commit fraud.

ATTENDANT RESPONSES TO FRAUD RISKS IN THE COVID-19 PANDEMIC ERA

Watching Out For Fraud Risk Factors

Auditors are required to obtain a concise understanding of the entity and its environment, including internal controls in order to be able to identify and be abreast with the various risks of material misstatement due to fraud. The potential of fraudulent financial reporting relative to fictitious

revenue and improper revenue recognition schemes should remain on the Auditor's radar while performing risk assessment procedures in the current environment (Thorps & Harding, 2020). However, some risk factors common to organisations in the COVID-19 pandemic regime as opined by Deloitte (2020) have been categorically presented below:

Risk factors associated with Pressure

a. Pressure to sustain the company's going concern status amid unfavourable performance picture.
b. Pressure to pay dividends and thus maintain distributable reserves.
c. Pressure to continue to pay employees and suppliers.
d. Pressure to meet bank and other covenants.
e. Financial pressures on individual employees due to loss of jobs, pay-freezes/cuts, unpaid leave, no bonuses or promotions.
f. Pressure to report all bad news now and make unnecessary write-offs that can be wrongly attributed to COVID-19. Industries (travel, hospitality, retail) that have been impacted more severely by the economic impact of COVID-19 will see increased pressure to commit fraud.

Risk factors associated with Opportunity

Changing and dynamic working patterns introduced in response to the COVID-19 pandemic outbreak may lead companies to alter usual and existing internal controls in order to allow commendable room for operations to continue.

Typical and notable examples are:

i. Daily approval of journals or other financial decisions may change when key officers of the company are off work.
ii. Need to increase system access rights for employees becomes imminent to allow remote working;
iii. Need for documentation requirements may be reduced.

While these may likely disrupt pending fraud schemes originated in response to existing internal controls in the organization, it may equally cause existing fraud schemes that exploited such existing loopholes in the organization to surface. Management should therefore be alert to existing frauds, not just the new ones yet to explode.

Risk factors associated with Rationalisation

Asmuch as employees do not wish to be caught in or associated with any fraudulent act, there are actually some employees that view the COVID-19 pandemic outbreak and the inevitable changes in the business environment accompanying it as rare and long awaited opportunities to commit fraud. This category of employees believe that they are less likely to get caught as the current disruption in the corporate environment will no doubt draw management's attention to other pressing areas of the company.

Risks factors associated with Manipulation

Altering accounting records and supporting documentation is potentially easier when much of the workforce work remotely as is the case in the COVID-19 pandemic regime. For instance,

a. Forecasts may be edited to produce favourable answers and avoid impairments or covenant breaches.
b. Transactions may be changed to avoid unfavourable impact on the statement of financial position or income statement. A notable example is changing the useful economic life of assets.
c. Digital copies of supporting evidence may be altered as people have more time and space to do this at home.
d. Changing cash flow forecasts to continue as a going concern.
e. Failure to provide for loss making contracts
f. Failure to impair goodwill or other intangible assets that are no longer supportable
g. Missing provisions or write-offs of bad debts.
h. Inappropriate capitalisation of expenses as tangible or intangible assets

i. Manipulating ratios to avoid breaches of covenants.
j. Manipulation of alternative performance measures and other key performance indicators
k. Manipulating forecasts and ratios to attract new capital finance or short term loans.
l. Manipulating results to qualify or earn external funders approval.

Risks factors associated with Misrepresentation

In the current COVID-19 pandemic environment, entities may wish to misrepresent the true position of the company. This may include:

a. Omission of vital information that readily alters Reader's view of the performance of the company. Failure to disclose the breach of a loan covenant or the loss of material contracts is a typical example.
b. Concealment of related party's transactions.

Risk factors associated with Misappropriation

In view of the prevailing dynamic business environment that has emerged in response to COVID-19 pandemic, risk of theft of valuable, marketable inventory or fixed assets will likely be on the increase. Where sites are not staffed to their usual levels, physical security may be reduced creating an opportunity for theft. The ENDSARs situation in Nigeria, though not related to business setting, which led to the break into warehouses where palliatives were hidden and packed is a typical example. Examples likely risks to look out for may include:

a. Unusual write-off of inventories.
b. The disposal of company's Assets without any proceeds collected.
c. New suppliers that have not gone through appropriate vetting processes
d. Purchasing staff collusion with suppliers leading to inflated pricing to the company (to cover bribes to purchasing staff)
e. Payments to persons not on the approved list of suppliers.
f. Observed unauthorized intervention in existing payment details of a customer's account to divert payments.
g. Payments to related parties, or members of staff outside of payroll.

Changing Organisation's views and attitude to Cyber and financial crimes

The continuous market and technology development prompted by a more commendable embrace of electronic commerce (e-commerce) in the COVID-19 pandemic era, has provided intending fraudsters with new scenarios and new methods to carry out fraudulent practices. Increase in internet activities across the globe and consequent rise in the adoption of mobile apps as modern means of executing business and non business transactions cum activities has also created opportunities and enabling environment for cybercriminals to thrive.

Cybercrime poses a unique set of threats to businesses and government worldwide. With millions of people across the globe now able to work remotely even from home, the risk of cyber threat such as phishing attacks and business email compromises has substantially increased (Luis, 2020) as these cybercriminals intensify effort to take advantage of the opportunities that vulnerable organisations with weak firewalls present. An April 2020 survey by the Institute of Internal Auditors (IIA)'s Audit Executive Centre revealed that 40% of professional Accountants studied as respondents have equally directed their internal audit functions on cybersecurity. Circulation of suspicious business links for customers' click, reoccurring calls and text messages demanding for customers' confidential transaction IDs, send out of large volume of phishing email lures requesting a click on link attached to enjoy or access free Kits or business offers, calls from imposters confirming customers Bank Verification Numbers (BVN) and requesting such customers to forward to the caller or designated phone number a personal identification number (pin) sent to the targeted customer's phone number, calls from suspected cyber criminals who confirms some digits of a customer's debit or credit

card but requesting the customer to call out the remaining numbers on such cards, design and registration of malicious domains such as new websites for dissemination of business related information to unsuspecting victims, spread of a very large portion of unverified harmful information on all social platforms, immediate response to a 'repost or share' prompting that could possibly circulate commendable number of misinformation from the comfort of the room et cetera, are a few cybercrime techniques presently on the increase in Nigeria.

Greater number of cyber-attackers now has access to multitude of individual and organizational social media accounts through which accounts of well-respected persons and businesses within the international community (Boismenu, Elbanna, Ben Rejeb& Farrag, 2020) are used to circulate misleading information so as to add credibility to false information being spread across different platforms. Hushpuppi, a Yoruba born Nigerian, as a typical example, is a popular cybercriminal arrested in June/July 2020 in the United States of America by the FBI for using such techniques in hacking into unsuspecting persons' emails and social media accounts, while rubbing his numerous victims off more than US$400 million.

For effective conduct of investigation in entities whose activities are internet-based and electronically inbuilt, professional Fraud Managers must acquire formidable IT skills that are consistently upgraded on timely basis in response to visible changes likely to overtake the business environment due to stiff competition and dynamic policies of the government. This entails that Business owners and Forensic Accountants must maintain a close oversight on the corporate environ so as to timely discover new technological entrants, understanding their relevance and possible consequence in the event of possible misuse by erring employees or management team members of organisations, and devise a reliable proactive counter measure(s) towards forestalling such predicted criminal efforts. In other words, an Oversight Regulator should not only be seen to be skeptical while discharging his duties, he must be predictive in character. Such professionals go further beyond the certificate acquired, qualifications held and prior exposures to train their minds on how to read and interprete the lines in an existing or looming cybercrime scene in order to rightly perceive the possible risk factors in an entity's Information Technology (IT) e-systems which could lead him (as an Investigator) to the secret domain or operating environment of the unknown cybercriminal(s). Businesses must enlighten their employees not accept instructions via phone from an unfamiliar person, not to allow or pave room for possible circumvention of existing internal control measures due change in mode of work, not to click on links or open documents that bear resemblance of those of the organization without first prior confirmation of the same from authorized peron(s). In view of this, business organisations are expected to provide clear instructions to their employees especially those working from home and keep them updated on developments from time to time. Other new facets of financial or cyber crimes are imposter scams, investment scams, products scams et cetera (Deloitte, 2020).

Understanding the Contemporary Business Environment in the COVID-19 Pandemic Era

With salary cuts and reductions currently ravaging the welfare of employees and the consequent elimination of bonuses and other forms of compensation, employees will be forced to find alternative means of replacing these wage-lost in order not to give room to further deterioration of their standard of living. This is more as over 90% of all significant theft losses to businesses come from employees. Every year, businesses lose over US$50 billion as a result of employee theft (note that Cash, property, or merchandise are targets of employee theft).

In other words, having adequate and reliable insight into the relationship between fraud and the prevailing business model of a corporate organization in economic downturns is considered very essential for rapid result-oriented response

purposes. The onus lies more with business organizations to evaluate and assess areas of its operations that are most vulnerable to fraud as a result of numerous changes that has occurred in the global and domestic corporate environments in response to the COVID-19 pandemic outbreak, getting to know their employees better towards understanding possible avenues or operations that could motivate them into unethical financial actions or wrongdoings. Although Hushpuppi may have been arrested in the United States of America, this does not negate the fact that his likes may have been recreated four hundred (400) fold across the globe since his arrest. The implication is that businesses internet/corporate firewalls are no longer considered safe in this era of rise of sophiscated technologies.

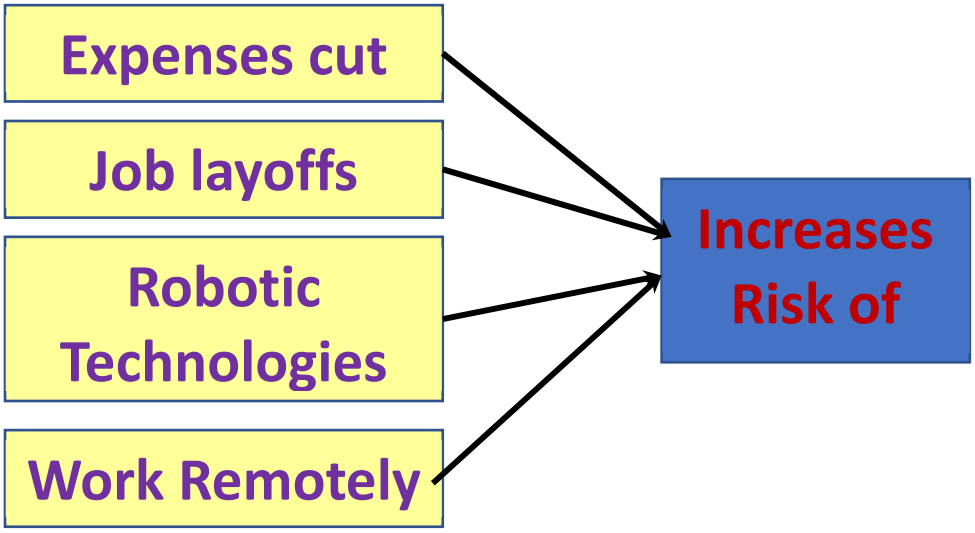

Figure 4: Spurs of fraud in the COVID-19 pandemic era
Source: Authors' concept.

Business organizations need to understand the current situation of the business while figuring out major drivers in the organization mostly impacted on by the after-effcet of the COVID-19 pandemic. Prevalent situation such as failure of Management to meet financial target for two to three quarters in 2021, top management's prioritization of organisation's operations and financial performance at the expense of fraud risk mitigation, continued decrease in periodical profit margin of the organization especially where Executive Directors compensation is tied to such performance, persistent decrease in organizations annual budgets, et cetera are equally pressing but dominant post COVID-19 pandemic factors currently engulfing many organizations globally. Adequate knowledge of these will also enable business organisations to identify with ease, indicators of possible fraud occurrence. And this helps improve such organisation's performance of fraud controls and effective risk management processes.

Upholding the Integrity of Financial Technology

With about 59.5% of the world population having access to the internet and more consumers driven by convenience shopping, the global retail ecommerce sales are projected to reach US$4.9 trillion by 2021 even as global payment fraud is on the rise and is estimated to cost customers and businesses about US$40.62 billion fraud losses by 2027 (had tripled from US$9.84 billion in 2011 to US$32.39 billion in 2020).

Financial Technology otherwise known as FinTech is an amalgamation of finance and technology that undoubtedly improves business conducts and financial transactions globally. This innovation has

also led to the rise of Financial Technology (FinTech) companies other than Commercial Banks that have been nicknamed Market Disruptors (FinTech firms compete with registered Commercial Banks and also deviate from the traditional recognised system of bank hall commercial trade and banking. Accordingly, FinTech is creating significant and sustainable opportunities that are growing daily globally due to the mass ownership of mobile phones and access to internet worldwide. The implication is that with FinTech which services includes mobile money, many people and businesses will maintain increased access to financial services. Countries like Ghana, Kenya, and Myanmar are currently enforcing measures to lower cost and increase patronage/utilization of digital transactions. Other countries like Namibia, Peru, Uganda, and Zambia where difficulties of accessibility to banking networks has not been completely overcomed, have embraced mobile money networks for relevant transactions (Sahay,Allmen,Lahreche, Khera, Ogawa, Bazarbash and Beaton, 2020). Tax authorities in Nigeria, Kenya, and Namibia are presently maximizing the benefits of FinTech for tax returns filling purposes.

It is worthy to note that the advent of this modern technology readily aids financial institutions to achieve efficiency and adequate cost savings as it supports zero paper usage and self service by way of less human intervention (Adedipe, 2020). In developing countries for instance, Financial Institutions, Telecoms and Technology(Tech), Bricks and Mortars firms currently deploy mobile banking apps, e-payment platforms and Point of Sale (POS) terminals to boost consumers services in the form of money transfers, roadside cash withdrawals and timely payment for goods and services from the comfort of their homes. This has helped businesses strengthen their drive for financial sustainability amid improved customers' satisfaction. But all these are not without uprising challenges to businesses.

FinTech is feared to promote certain level of risk accompanying its implementation as its adequate deployment equally exposes adopting countries, businesses, companies, and individuals to tendencies of cyber attack, fraud, money laundering, and terrorism financing. Adedipe (2020) also agrees with this view stressing further that prevalence of Know-Your-Customer (KYC) checks and regular due diligence that are largely void of physical human contact or interaction poses some difficulties in minimizing the illegal activities of cybercriminals especially in the area of personalities identities verification (PIV) as FinTech readily erodes the need to physically meet with consumers. This is readily linked to the rising incidence of cyber related cases across the globe especially in developing countries like Nigeria where millions of US Dollars have been stashed away from businesses and individuals by unsuspecting persons since the advent of COVID-19 pandemic which ideally, discourages social or business gatherings and promotes online gatherings/meetings, contacts, payments and seamless services.

In the wake of COVID-19 pandemic restrictions imposed world in 2020, the use of PoS witnessed a boom as many customers patronised the operators during the shutdown of commercial banking activities. Available statistics from the Nigeria Interbank Settlement System (NIBSS) revealed that the value of January and June 2021 transactions through PoS terminals in Nigeria stood at N3.01 trillion. This represents about 50% increase when compared to N2.03 trillion recorded value of transactions in year 2020.

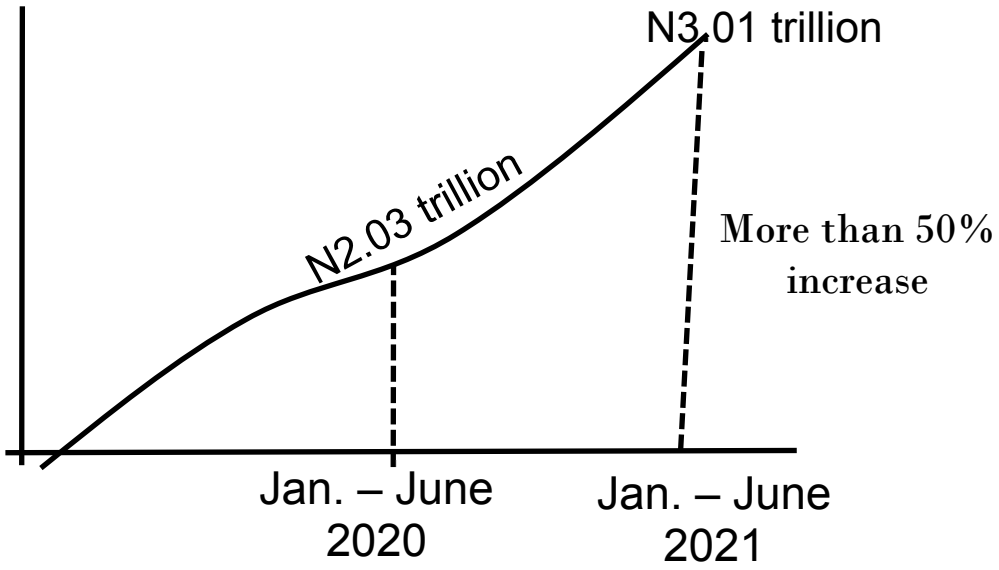

Figure 5: POS usage trend in Nigeria
Source: Authors' concept

However, statistics from the Nigeria Deposit Insurance Corporation (NDIC) indicated that online fraud has become a growing concern for investors in the financial services sector, with a hefty loss of N15.5billion in 2018. The banking sector lost a total of N12.30billion between 2014 and 2017. About 89 per cent of all the fraud happened through electronic channels. Furthermore, the 2020 NIBSS report showed that the banks lost N3.5billion between July and September 2020 as a result of the activities of hackers, cyber-criminals and other malicious actors. The loss represents 534% rise from the same period in 2019 when it was N552 million. Transactions over the phone during this period in 2020 accounted for a loss of N410 million or 11.7% of the entire loss (SunNewsOnline, 2021).

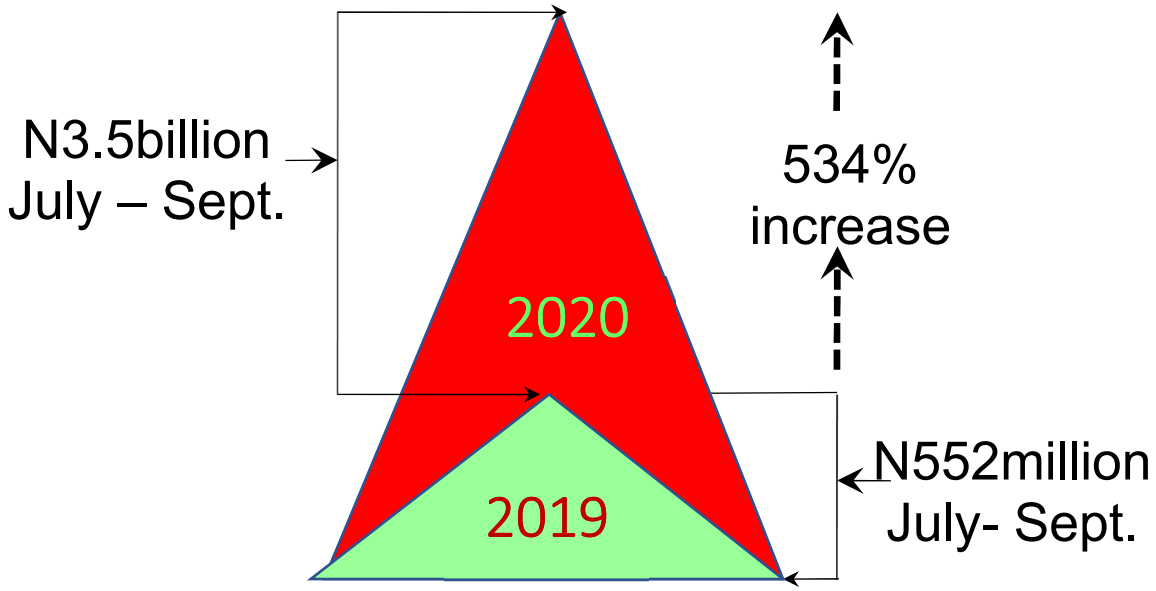

Figure 6: Nigerian banks' Loss trend to cyber attackers
Source: Authors' concept

One of such popular internet based fraud is called Point of Sales (PoS) fraud. PoS fraud could be physical such as when a chip is inserted into the POS device by a local criminal, or it could be digital where the PoS system is infected with card number-stealing malware. There is also the ever present threat of card skimmers and shimmers, which are devices that can capture card data from EMV chip cards. Card-Not-Present (CNP) fraud appears to much more prevalent than Card oriented fraud on Pos, ATM et cetera. CNP occurs when a credit card number is used online for a transaction over the phone or in another manner without the physical card in use and without the prior knowledge of the Credit Card owner. A study found that retailers could lose as much as US$130 billion from CNP fraud by 2023 as it is 81% more likely to occur than POS fraud.

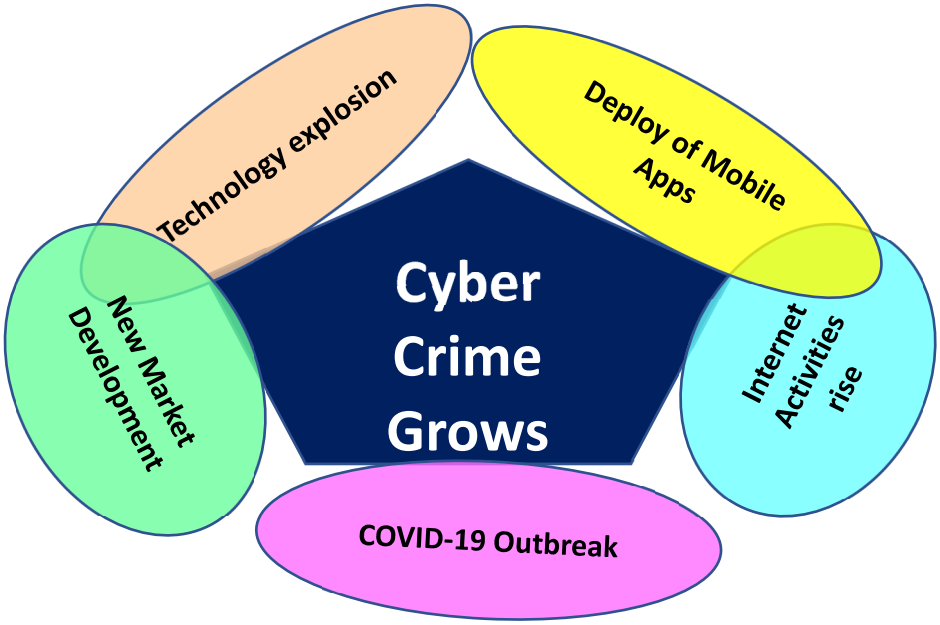

Figure 7: cyber and financial technology crimes motivational factors
Source: Authors' concept.

To minimise this fraud incidence, the operators are advised to learn to utilise point-to-point encryption (P2PE) solution to safeguard PoS data. Without P2PE, it is near impossible to guarantee that payment data will remain secure from customer's smart phone to its destination. For CNP, businesses could require their Consumers to insert the card verification number before proceeding with any order. Taking up an insurance policy against cyber attack is equally advised, especially for business owners. Apex Regulatory Banks and its licensed Commercial banks must take to research and brainstorming to come up with more sophiscated measures to check these rising stigma.

Restoring Misplaced Values

Strong campaigns should be consciously pursued at corporate organizational level to re-awaken these values. Staking commendable seriousness to this is highly recommended to organisations. This is more as reliance on the intervention of anti-graft agencies may not yield the desired result as these agencies seem to be rigged with challenges that hamper their performance, issues ranging from funding inadequacy, undue interference by political leaderships, independence of objective, transparency and systematic performance. In Africa for instance, factors such as Judicial weakness, Legislative weakness, shielding effect of the

immunity clause, overbearing effect of partisan politics et cetera remain enormous challenges to surmount.

1. **Selflessness:** Holders of office in public and private establishments should act solely in the interest of the investing public and the citizenry. Financial gains and other benefits derivable by them or for their family or friends should not serve as the drivers behind services.
2. **Integrity:** The absence of this very principle among corporate employees and public office holders in Nigeria has actually been one of the foundational bane of fraud and corruption in many developing countries like Nigeria. Occupants of these positions/offices are not also expected to place themselves under any form of oath or financial obligation to other individuals or organisations that might seek to influence them in the performance of their official duties; in politics, for instance, political god fathers or king makers.
3. **Objectivity:** In discharging corporate or civic responsibilities especially in making appointments, awarding contracts, or recommending individuals for rewards and benefits, choices should be made on merit without any form of sentiments attached.
4. **Accountability:** Office holders and employees in the position of administrative leadership or governance are accountable for their decisions and actions, and must submit themselves to whatever periodic scrutiny or oversight is considered appropriate.
5. **Openness:** Managers of corporate organisations or persons in Public leadership should be as open and transparent as possible, especially in matters affecting decisions and actions made and taken on behalf of the organisations they represent. Unbiased explanations should be given when relevant and needed in issues demanding sensitive decisions and actions.
6. **Honesty:** Employees and public servants have the duty to declare any private interests relating to their duties and to take constructive steps to resolve such in a manner that protects the general interest of the investing and non investing public. The silent attitude of the Federal and Kaduna State governments in Nigeria to the Kaduna South killings that claimed many lives unchecked over a long period, is typical example of dishonesty in the handling of organizational affairs.
7. **Leadership:** Leadership by example is the only true sure means of implementing the above enumerated principles in corporate and non corporate governance structure.

WAY FORWARD

The monthly salaries and allowances of employees should be consonant with the prevailing cost of living, quality and quantity of work done, inflation rate, and the prevailing exchange rate (value of the currency) during the period in which the salaries are paid. It is enough pressure for employees to to earn in year 2021 at an exchange rate of N520 to US$1, the same salary they were paid ten years ago when exchange rate was N280 to US$1. A situation whereby salaries structure remain the same amid tremendous and continuous rise in the affected nation's inflation rate from single digit to double digit could motivate an employee to commit fraud. The purported plan of the federal government to remove subsidy with effect from February 2022, though later cancelled, would have done more harm than good to those in governance and the corporate environment given the economic and poverty state of the nation.

Half year interim audit by external professional Auditor should be embraced consciously and willingly by all corporate organisations. Observance of top management oversight role should be prioritized too to commendably debase all tendencies of internal control override by management team members of the organization.

With good governance structure, sense of decency and patriotism as well as outright respect for the rule of law in place, prevalence of finance mismanagement and ineptitude will be tamed effectively.

Organisations need to revist their administrative cost of operating the business in the COVID-19 pandemic era. This is in view of the fact that many organisations currently deploy a mix of hall-based and remote-based work pattern so that a few staff work at designated office space while others work from home on a daily target.

Solid controls that permit auto stock taking should be put in place for the effective monitory of trading organisations' e-stocks trading online. Commendable real time checks should also be observed by e-audit professionals in the employment of organization to enable the organisation forestall possible intrusion of unsuspecting persons into the e-trading activities of the organization and consequent unnecessary cash outflows and loss or theft of e-stocks. This, when properly linked to e-commerce activities, will also boost customers' confidence and enhance their sense of security in the online markets without fear of being hacked or robbed.

It is pertinent that Small and Medium Entreprises adopt and fully implement electronic system of accounting and financial reporting towards completely shutting out risks associated with the manual system of accounting that has proven to be complex and mistakes-oriented as the volume of daily transactions and activities in the businesses increases. This will also pave room for improved audit trail, tax assessment and complete audit overhaul of organisation's electronic accounting data from a remote area at any point in time without the need for the physical presence of the audit professional.

There should be timely procurement, installation and implementation of digital forensics equipment in relevant internal audit and security units of government Ministries, Departments and Agencies for effective and adequate e-audit trail performance, detection and investigation of various cyberattacks on private and public owned establishments. Moreso, cybercrime investigations specialized interventions should be encouraged to help boost effective prevention of further occurrences. This entails that digital forensics response to various cybercrime scenes should also take the centre stage as part of the priorities needy of Legislative review and considerations towards achieving effective oversight and data tracking.

Although the National Assembly in Nigeria has passed the second reading of a bill for the creation of Chartered Institute of Forensics and Certified Fraud Examiners of Nigeria (CIFCFEN), a more enabling environment is needed for entreprises' maximum utilization of forensic accounting professional services in Nigeria. Installation of standard internet-based digital infrastructures in developing countries in Africa readily enhances the continents' ability to meet up with sophiscated global technological innovations presently being used to deter and discourage the activities and growth of financial and cyber crimes in developed countries. This will also commendably help to curtail possible inter and tntra movement of cyber criminals between suburbs and cities across the African continent.

REFERENCES

Adebowale, Y. (2021). Nigeria's Untenable Rising Debt Profile, July 17, Available at https://www.thisdaylive.com/index.php/2021/07/17/nigerias-untenable-rising-debt-profile/

Adedipe, A.A. (2020). FinTech and Anti-Money Laundering Regulation in Nigeria, *Strachan Partners News Letter*, 1 – 3.

Adegbesan, E. (2020). PoS fraud poses nightmares to bank customers, *Vanguard Nigeria*, November 2, Available at: https://www.vanguardngr.com/2020/11/pos-fraud-poses-nightmares-to-bank-customers/

Boismenu, P., Elbanna, M., Ben Rejeb, S. & Farrag, N. (2020). COVID-19: Cyber Threat

Analysis, *United Nations Office on Drugs & Crime*, May 10, 1 – 15.

Deloitte (2020). Covid 19 and Fraud Risk: Managing and responding in times of crisis, file:///C:/Users/hp.com/Documents/My%20ARTICLES/FRAUD%20Fact%206.pdf

Financeonline (2021). 57 Crucial eCommerce Fraud Statistics for 2021: Types, Cost & Protection Data, accessed September 13, Available at: https://financesonline.com/ecommerce-fraud-statistics/

ICAEW (2021). Reactive firms are victim to rocketing cost of financial fraud, ICAEW Insights, 14 July, Available at: https://www.icaew.com/insights/viewpoints-on-the-news/2021/jul-2021/reactive-firms-are-victim-to-rocketing-cost-of-financial-fraud

Inyang, E.E., Peter, Z., & Ejor, N. O. (2014). The Causes of the Ineffectiveness of Selected Statutory Anti- Corruption Establishments In Fraud Prevention And Control In The Nigerian Public Sector, *Research Journal of Finance and Accounting*, 5(5), 163-170.

Luis, N. (2020). A Blueprint to Managing Corporate Fraud Risk during a Pandemic, *the Institute of Internal Auditors*, 1 – 13.

Okoye, E. I. (2000), The Nigerian Debt Problem: Causes, Consequences and Option, African Banking & Finance Review, 1 (1), June: 57 – 64

Okoye, E. I. (2001). Management of Stress in a Depressed Economy, *Journal of Management Sciences, 5* (1) January: 71 – 78

Okoye, E. I. (2005). Overcoming the Fear of the Rainy Day: A Look at the Available Viable Opportunities, *OKO Journal of Business Studies, 4* (1): 35 – 46

Okoye, E. I. (2006), Understanding the Behavioural Theory of Fraud: The Accountants' Perception of the Fraud Triangle, *The Certified National Accountant, A Quarterly Journal of* Okoye, E.I. (2015). Forestalling Corruption in the Public Sector: The Use of Professionalism and Value development, A paper presented at the Annual Conference of the Nigerian Accounting Association that held in Bayelsa State, 21 – 22 May.*Association of National Accountants of Nigeria, 14* (1) January - March, 40 – 53.

Okoye, E.I. (2015). Forestalling Corruption in the Public Sector: The Use of Professionalism and Value development, A paper presented at the Annual Conference of the Nigerian Accounting Association that held in Bayelsa State, 21 – 22 May.

Okoye, E. I. & Akamobi, N. L. (2009).The Role of Forensic Accounting in Fraud Investigation and Litigation Support, *The Nigerian Academic Forum*, *17*(1), 39 – 44.

Okoye, E. I. & Akenbor, C. O. (2009a), A Critical Analysis of the Fraud Triangle for Sustainable Development in Africa, *The University Advanced Research Journal, 1*, April-June, 1 – 7.

Okoye, E. I. & Akenbor C. O. (2009b), Forensic Accounting in Developing Economies Problems and Prospects, *The University Advanced Research Journal,1,* July - September, 1 – 13.

Okoye E. I. & Gbegi D.O. (2013a). An Evaluation of Forensic Accountants to Planning Management Fraud Risk Detection Procedures, *Global Journal of Management and Business Research, 13* (1), 74 – 90.

Okoye, E. I. & Gbegi, D. O. (2013b). Evaluation of the effect of fraud and related financial crimes on the Nigerian Economy, *Kogi Journal of Management, 5*(1), 200 – 223.

Okoye, E. I. & Jugu, Y. G. (2010). An Empirical Investigation of the Relevant Skills of Forensic Accountants in Nigeria, *Journal of Knowledge Management, 1*(2): 34 – 47.

Okoye, E.I. & Nwoye, U.J. (2015). Skeptically forestalling fraudulent financial reporting in publicly listed Manufacturing companies in Nigeria: The role of the Beneish Model, *Journal of Global Accounting*. 3(1), 35 – 44.

Okoye, E. I.& Okafor, B. E. (2006). The Complexity of Investigation Procedure in a Computer Related Embezzlement, *The Nigerian Accountant, 39* (1), January/March: 20 – 23.

Okoye, E.I. & Okaro S.C. (2012), Forensic Accounting and Audit Expectation Gap - The Perception of Accounting Academics, Available at: http://ssrn.com

Okoye, E.I. & Udeh, F. N. P. (2009a). Money Laundering and Financial Crimes in the Banking Industry; Government and Accountants in Nigeria, *National Journal of Banking and Finance, 1* (1), 67 – 79.

Okoye, E.I. & Udeh, F.N.P. (2009b). Fixed Asset Management in Public Sector Organisation; Economic Impact on a Developing Country, *National Journal of Banking and Finance, 1* (1), 9 – 16.

Sahay, R., Allmen, U.E., Lahreche, A., Khera, P., Ogawa, S., Bazarbash, M. and Beaton, K. (2020). The Promise of Fintech: Financial Inclusion in the Post COVID-19 Era, International Monetary Fund, No. 20/09, 1 – 83.

Texas Wesleyan (2020). Accounting: Forensic/Fraud Professional Organizations, Texas Wesleyan Univesity, accessed on October 25. Available at: https://txwes.libguides.com/c.php?g=825801&p=5895512

Thorps, D. & Harding, T. (2020). Auditing fraud risk during a pandemic, *Journal of Accountancy*, December, Available at: https://www.journalofaccountancy.com/news/2020/dec/auditing-fraud-risk-during-coronavirus-pandemic.html

SunNews (2021). Dealing with PoS fraudsters, *Sunnewsonline*, September 4, Available at: https://www.sunnewsonline.com/dealing-with-pos-fraudsters/