Global Scientific JOURNALS

GSJ: Volume 9, Issue 1, January 2021, Online: ISSN 2320-9186
www.globalscientificjournal.com

Detection, Prevention and Control of Digital Fraud in Nigeria

Muhtar H.Alhassan *

Department of Computer Science, National Open University of Nigeria
Abuja - Nigeria
* malhassan@noun.edu.ng

***Abstract*—Nigeria is blessed with abundant resources both human and material. Since independence in 1960, attempts have continuously been made to harness these resources to ensure steady and persistent development of the economy. Little has been achieved however, as Nigeria has remained underdeveloped by most economic indices. Much of the blame for this stagnation can be placed squarely on fraud, corruption, and other forms of economic mismanagement. Current realities dictated by digital transformation make it imperative to employ modern management techniques to develop an economy that can thrive in the new highly competitive economic environment. This paper takes a particular look at the increased risks of fraud and the strategy of mitigating them in the wake of the impending digital transformation of the economy in Nigeria.**

I. Introduction

Fraud has been defined as irregularities involving the use of criminal deception to obtain an unjust or illegal advantage. Fraud is a global problem and poses more threats to society with the arrival of the information revolution that is sweeping the world. Criminologists have formed a consensus that fraud conforms to the ubiquitous Fraud Triangle, which is universally accepted in almost every setting in which fraud is described or analysed.[1] The triangle states that individuals are motivated to commit fraud when three elements come together. These are:

1) some kind of perceived *pressure*
2) some perceived *opportunity* and
3) some *rationalisation* that the fraud is not inconsistent with one's values.

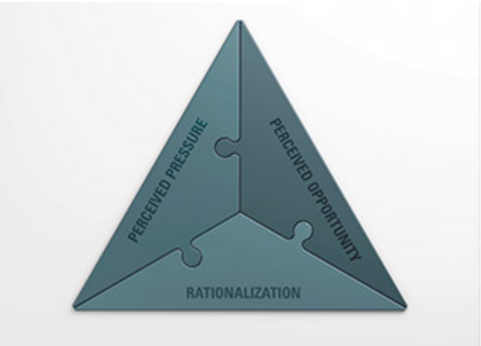

Fig. 1. *The fraud triangle[1]*

An alternative approach is to assert that three *ingredients* are required to actualise a fraud.These are: *will*, *opportunity*, and *exit* (WOE).[3] The *will* to commit fraud by the individual is influenced by such factors as greed, poor remuneration, and apparent indifference by the society towards fraudulently acquired wealth. The *opportunity* to commit fraud is enhanced by poor internal control, and generally bad management. Finally, *exit* refers to the confidence, justified or not, of the individual that an escape from punishment is available on executing the fraud or attempting it.

II. Categories of Fraud

Typical types of fraud that are rampant in Nigeria include:

- Falsification of figures
- Forgery of authorised signature
- Ghost workers
- Pre-mature writing-off of assets
- Over-invoicing
- Impersonation
- Double pledging
- Digital Fraud

The last item on the above list, *Digital Fraud* is a new phenomenon brought about by gradual digitalisation of the economy. Digital fraud is a problem businesses world-over are facing since the advent of e-commerce in the 1990s with its threat continuously increasing. Losses from fraudulent activities increased from 51% in 2017 to 57% in 2019, and according to PwC, these crimes cost companies $42 billion in the last 24 months.[6] Some of the reasons for increase in digital fraud include:[6]

1) Economic chaos triggered by the global COVID-19 pandemic.
2) Significant changes in the e-commerce landscape.
3) Huge rise in online Payments.
4) Increased digital banking services.
5) Pressure due to new consumer expectations.
6) Appearance of increasingly sophisticated fraud tactics
7) Poorly defined legal jurisdiction for cross-border fraud.
8) Increased deployment of digital technology in business

III. System Vulnerability

In a manually managed information system, data about individuals and organisations are maintained and secured as paper records dispersed in various organisational units. In computerised information systems on the other hand, data is concentrated in computer files that can potentially be accessed more easily by large numbers of people and in most cases even by groups outside the organisation.

The weaknesses of manually managed systems include:

1) Poor security controls
2) Absence of detailed operational procedure
3) Ease, with which manual, paper-based documents and records can be hidden, stolen, tampered with, or destroyed. In many cases paper documents are burnt by arson to cover evidence of frauds.

As businesses and organisations increasingly depend on computerised information systems, they come to rely on highly concentrated data in electronic form that is vulnerable to destruction, misuse, error, fraud, and system failure. Computerised systems are particularly vulnerable to many more kinds of threats than the manual type for reasons that include:

- complexity and size of computerised systems, which make them difficult to replicate manually
- *invisible* nature of computerised procedures, which makes them difficult to audit

IV. ICT-specific security issues

Security is of particular importance in any system that involves an electronic network. The organisation's network carries a great deal of data, much of which is sensitive or proprietary. These include profit reports, product development information, pricing data, marketing plans, sales contacts, and so on. As organisations establish intranets and get linked to the Internet, the risk of fraudulent attacks from mischief-makers within and outside the organisation arises. Thus, when organisations become so dependent on computerised information systems, they must take special measures to ensure that such systems are properly controlled. On-line systems and those using telecommunications are particularly vulnerable as data and files can be immediately and directly accessed.[4]

Telecommunications networks enable information systems in different locations to be interconnected. The potential for unauthorised access, abuse, or fraud is thus not limited to a single location but can occur at any access point in the network. Wireless networks using radio-based technology add more vulnerability as radio frequency bands are easy to scan.[4]

V. Hacking

Hacking is defined as gaining unauthorised access to computer networks for profit, criminal mischief, or personal pleasure. Hackers have been known to break into information systems of organisations to steal information, temper with data, introduce viruses, or crash down the systems by flooding them with massive unwanted e-mails. Many organisations are thus, reluctant to deploy Cloud solutions for fear of hackers' ability to use latest technology to break into their computer systems via the Web. It must be pointed out however, that the biggest threat to information systems is posed not by hackers but by authorised users. The end-user is usually the weak set link in the computing network and hackers usually exploit poor computing habits such as poor choice of passwords, unattended sessions, and others to gain access to otherwise well protected systems.

A. ”Nigerian Prince” Email scam

This scam is popular among the so-called ”Yahoo boys”, who are usually in their twenties and use social media for both communication and operations. Typical schemes here include:

- *Advance Fee Fraud.* In this case the fraudster pretends to have an issue trying to transfer tremendous wealth recently obtained either from extremely rich family estate or by winning a lottery. The intended victim is then asked to provide account details through which the funds can be moved out of the country. The ultimate aim is to obtain the victim's bank details and /or make the victim part with some money in form of service charges for the anticipated transfer.
- *Stranded-traveler scam.* This scam relies on the sympathy of the victim to a made-up story about a disaster seemingly affecting the scammer so that some financial assistance is offered.
- *Romance Fraud.* Here, the scammer builds up a romantic relationship with the victim, and subsequently uses that to request for financial support.

B. BEC Hacking

Business Email Compromise hacking is the latest form of hacking which has Nigeria as its epicentre. In this type of digital crime, the scammer impersonates a CEO or other business executive and then tricks a victim into sending them money. Globally, BEC hacking causes the loss of over US$9bn annually and 50% of the scam originates from Nigeria.[5] This scam requires some basic hacking tools such as key loggers and remote access Trojans or RATs, usually procured from underground forums.

VI. Coping Strategies

Obviously, the strategies for confronting fraud in all its forms will have to address the issues of will, opportunity and exit mentioned earlier. To suppress the individual's will or motivation to embark on fraud there must be improvement in the general condition of living, awareness, literacy level, sense of responsibility, etc among the populace. This will only reduce the temptation to defraud but cannot eliminate it completely.

An important deterrent to fraudulent practices is the establishment of controls that limit the opportunity to commit fraud and block the chances of getting away with successful or even attempted fraud. Our focus will therefore be on such measures based largely on ICT that deter individuals and groups from committing fraud and other criminal mischief.

A. Controls as deterrents

Proper control includes all the methods, policies, and organisational procedures that ensure the safety of the organisation's assets, the accuracy and reliability of its accounting records, and strict adherence to management standards. For a computerised information system there are two main categories of controls: general controls and application controls.

1) General Controls: General controls handle overall design, security and use of computer programs and files for the organisation. These include administrative controls, physical hardware controls, system software controls, data file security controls, computer operations controls, and so on.

- *Administrative controls* are the formalised standards, rules, procedures set up to ensure that the organisations general controls are properly executed and enforced. These controls include segregation of functions, written policies and procedures, and supervision. Segregation of functions minimises the risk of errors and fraudulent abuse of the organisation's assets. Written policies and procedures establish formal standards for controlling the organisations operations. Here, accountabilities and responsibilities are clearly specified. Supervision ensures that controls are not bypassed or neglected.
- *Hardware controls* are used to ensure the physical security and correct performance of computer hardware. Software controls similarly ensure the security and reliability of computer software.
- *Data security controls* protect data files on storage devices like disks and tapes from unauthorised access, change, or destruction. Such data must be protected whether in storage or when they are being processed. In cases where data can be input on-line via a terminal, entry of unauthorised input must be prevented. Measures to ensure this include:
  - Physical restriction of terminals so that they are available only to authorised individuals.
  - Preventing those without a valid password from login on to the system
  - Developing additional sets of passwords and security restrictions for specific applications and transactions.
  - Maintenance of usage logs and records.

2) Application Controls: These are controls that are specific to computerised applications. Their focus is on the completeness and accuracy of input, updating and maintenance, and the validity of the information generated. Thus, application controls essentially consist of input controls, processing controls and output controls.

- *Input controls* are the procedures to check data for accuracy and completeness at the point of entry to the system. These controls include input authorisation, data conversion, data editing and batch control totals.
  - *Input authorisation* ensures that source documents are properly authorised, recorded, and monitored as they enter the computer system.
  - *Data conversion controls* ensure that input is properly converted into suitable form for entry into the system. Transcription errors are eliminated by keying input transactions directly into computer terminals or by using some form of source data automation.
  - *Data editing* is used to verify input data and correct errors prior to processing. Edit techniques used include reasonableness checks, format checks, existence checks, and dependency checks.
  - *Batch control totals* are established beforehand for transactions grouped in batches. These totals vary from simple document counts to totals for quantity fields such as total sales for the batch. The batch totals from transactions input are counted and batches that do not balance are rejected. For on-line real-time systems, entry control totals are reconciled with hard copy documents used for the input.
- *Processing controls* are required to establish that data are complete and accurate during updating. There are three main processing controls: run control totals, computer matching, and programmed edit checks.
  - Run control totals are the procedures for controlling the completeness of computer updating by generating control totals that reconcile totals before and after processing.
  - Computer matching is used to match input data to information held on master files.
  - Programmed Audit checks
- *Output controls* ensure that results of computer processing are accurate, complete, and properly distributed. Output controls include:
  - Balancing output totals with input and processing totals
  - Reviews of computer processing jobs to ensure that all jobs have executed properly
  - Procedures and documentation that specify authorised recipients of various output reports, checks, or other critical documents

B. MIS Audit

MIS audit is used to identify all the controls that govern the information system and assesses their effectiveness. The MIS auditor must acquire a thorough knowledge of operations, physical facilities, telecommunications, control systems, data security objectives, organisational structure, personnel, manual procedures, and individual applications. Data quality audit is carried out to ensure the accuracy and completeness of data in an information system. This is achieved by surveying end-users and data files either entirely or by random sampling techniques.

C. Legislation and Law Enforcement

Nigeria has a robust strategy for fighting fraud as evidenced by the establishment of several regulatory and enforcement agencies. prominent among these organisations are the Economic and Financial Crimes Commission, the ICPC, the

Nigeria Police, and NITDA. In the special case of cybercrime, there are several legislations that are targeted at confronting the perpetrators. NITDA has also developed a Data Protection Regulation aimed at safeguarding the rights of natural persons to data privacy and ensuring that Nigerian businesses operate under a just and equitable legal framework that is in tune with global best practice.

VII. Conclusion

As we adopt new technologies that pose new risks and new types of criminal mischief, it will be necessary to put in place legislation that spell out clear breaches of the law and the appropriate punishment for such breaches. Fraud detectives should be trained to use latest technology in detecting forgeries and irregularities. The tremendous computing and graphical capabilities of modern digital computers can be used in forensic analysis. An efficient well-equipped law enforcement outfit will have the ability to use modern technology in tracking down mischief-makers and prosecuting them with a high degree of success. Thus, there is the need to train and equip the police force in line with the challenges of the information age. Forensic laboratories should be furnished with the latest equipment and the police should have a comprehensive fully automated information system that spans the entire nation.

ICT can provide the police and other law-enforcement agents with the ability to confront even international fraudsters who are surely going to be a problem as the full impact of digitalisation begins to hit us.

References

[1] ALBERT, S.W.: 'Iconic Fraud Triangle endures: Metaphor diagram helps everybody understand fraud,' *Association of Certified Fraud Examiners, ACFE, July/August 2014* , https://www.acfe.com/article.aspx?id=4294983342

[2] ALHASSAN, M.H.: 'Information and Communications Technology in Fraud Detection, Prevention and Control'*Paper presented at the TIN-NACIMA Integrated Accord Workshop, Yankari Games Reserve, Bauchi, 2001* .

[3] HUR-YAGBA, Y.: 'Frauds in the Nigerian banking industry,' *Abuja Management Review, 2003*, **1**, (1), pp. 11-17

[4] LAUDON, K. C. and LAUDON, J. P.:'Essentials of Management Information Systems- Organisation and Technology', *Prentice Hall, New Jersey, 1997*

[5] TrendMicro: 'Is There a Budding West African Underground Market?' , *TrendMicro, 2017* https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/west-african-underground

[6] REYNOLDS, J.: "9 reasons digital fraud is on the rise"*Security Magazine, 2020* https://www.securitymagazine.com/articles/93912-reasons-digital-fraud-is-on-the-rise