WELCOME

Prof. Godwin Emmanuel, Oyedokun

HND (Acct.), BSc. (Acct. Ed), BSc (Acc & Fin), MBA (Acct. & Fin.), MSc. (Acct.), MSc. (Bus & Econs.), MTP (SA), PhD (Fin), PhD (Acct), FCA, FCTI, ACIB, ACS, MNIM, CNA, FCFIP, FCE, FERP, CICA, CFA, CFE, CIPFA, CPFA, ABR, CertIFR, FFAR

godwinoye@yahoo.com

+2348033737184, +2348055863944 & +2348095491026

Managing Partner

Oyedokun Godwin Emmanuel and Co

(Chartered Accountants & Tax Practitioners)

ELECTRONIC FRAUD: CYBERCRIMES AND INTERNET FRAUD PERSPECTIVES
WHAT ACCOUNTANT SHOULD KNOW

BY

PROF. GODWIN EMMANUEL, OYEDOKUN

BEING A VIRTUAL PRESENTATION AT THE INSTITUTE OF CHARTERED ACCOUNTANTS OF NIGERIA, IKEJA DISTRICT MEMBERS FORUM WEBINAR HELD ON

20TH FEBRUARY 2021.

PRESENTATION OUTLINE

- INTRODUCTION
- CONCEPT OF FRAUD
- CONCEPT OF ELECTRONIC FRAUD
- ACCOUNTANT AND ELECTRONIC FRAUD
- RELEVANCE OF ACCOUNTANT IN DETECTION AND CONTROL
- HOW TO PREVENT ELECTRONIC FRAUD
- CHALLENGES IN DETECTION AND CONTROL OF ELECTRONIC FRAUD
- CONCLUSION AND RECOMMENDATION

INTRODUCTION

- Fraud has progressed from being perpetrated by off the cuff impostors to being perpetrated by well thought out delinquency and racket rings that utilize urban ways and means to invade and gain into private organization, individual and financial institution account in a means to syphon funds.

- The advancement in the computer technology has led to the emergence of new crime activities via electronic means, however, current wave of economic globalization requires extensive application of ICT in carrying out financial transactions.

- As a result, e-commerce is seemingly assuming the center stage in the world of business as it has imparted sophistication in the way the global community carries out business transactions.

INTRODUCTION/2

- In addition, electronic money transfers have offered people with a reliable alternative of buying and selling items through electronic means. Purchase and selling of goods and services are currently being conducted at the comfort of one's sofa set in the house or on the office chair.

- This has been enhanced by the invention of e-payment services, in which buyers can purchase commodities via online connection, the so-called online shopping and send the payments to the seller through electronic money transfer means.

- With all these benefits, it is important to know that it is associated with high security pressures which has led to increasing concerns on cases of cybercrime threatens that tends to threaten trust and transparency in business and governments on a daily basis. The public in this regard increasingly expects greater openness about the ethical issues arising from cyber security breaches, and how personal data is protected.

- To this end, Accountant In their roles as value protectors and stewards need to be part of the solution when it comes to cyber security, whether they are advising their clients or working in a finance and accounting team, or in a broader strategic or operational role.

CONCEPT OF FRAUD

What is Fraud?

➢ Fraud is a broad legal term referring to dishonest acts that intentionally use deception to illegally deprive another person or entity of money, property, or legal rights.

- In committing fraud, perpetrators may be seeking either monetary or non-monetary assets by deliberately making false statements.
- For example, knowingly lying about one's age to obtain a driver's license, criminal history to get a job, or income to get a loan may be fraudulent acts.
- A fraudulent act should not be confused with a "hoax" a deliberate deception or false statement made without any intention of gain or of materially damaging another person. Perpetrators of criminal fraud may be punished by fines and/or imprisonment.

CONCEPT OF FRAUD/2

ELEMENTS OF FRAUD

1 MISREPRESENTATION OF A MATERIAL FACT

A false statement involving a material and pertinent fact must be made. The gravity of the false statement should be adequate to substantially affect the victim's decisions and actions.

2 REASONABLE RELIANCE BY THE VICTIM

The level to which the victim relies on the false statement must be reasonable in the eyes of the court. Reliance on rhetorical, outrageous, or clearly impossible statements may not amount to "reasonable" reliance.

3 KNOWLEDGE OF FALSEHOOD

The party making the false statement must know or believe that it is untrue or incorrect.

CONCEPT OF FRAUD/3

ELEMENTS OF FRAUD

4 INTENT TO DECEIVE

The false statement must have been made expressly with the intent of deceiving and influencing the victim.

5 ACTUAL LOSS OR INJURY SUFFERED

The victim suffered some actual loss as a direct result of their dependence on the false statement.

CONCEPT OF FRAUD/4

FRAUD RISK FACTORS

CONCEPT OF FRAUD/5

FRAUD RISK FACTORS

PRESSURE

- This explains the motivation that leads to unethical behaviors.
- To commit fraud can be personal, employment or external pressure and each of these types of pressure can also happen because of financial and non-financial pressure.

CONCEPT OF FRAUD/6

FRAUD RISK FACTORS

OPPORTUNITY

- This is created by weaknesses in the system that allow an individual to commit fraud; in the accounting field, this is called weak internal control.

CONCEPT OF FRAUD/7

FRAUD RISK FACTORS

RATIONALISATION

- Rationalization which is the last phase of the fraud triangle cycle is where the fraudster gives a reason for committing the crime that is acceptable to his or her internal or external range.

CONCEPT OF ELECTRONIC FRAUD

- The Internet could be defined as a connection of electronic gadget such as computers anywhere in the world via routers and servers.

- In a simple sense, it explains a connection that one person can have with another from any part of this planet to share information.

- However, the Internet is also an excellent tool for fraudsters. People do all sorts of fraudulent deals on the internet.

- It is easy for fraudsters to make their messages look real and credible, almost impossible for business people and investors to tell the difference between fact and fiction on the internet. Through this, many people have been defrauded and duped.

- Hence the term 'electronic fraud' refers to any type of fraud scheme that uses email, web sites, message boards to present fraudulent solicitations to prospective victims, to conduct fraudulent transactions or to transmit the proceeds of fraud to financial institutions or to others connected with the scheme via the use of electronic gadget like computer and mobile phones.

CONCEPT OF ELECTRONIC FRAUD/2

TYPES OF ELECTRONIC FRAUD

SPAM

- Spam is a generic term used to describe electronic ‘junk mail’ or unwanted messages sent to your email account or mobile phone.

- These messages vary, but are essentially commercial and often annoying in their sheer volume. They may try to to trick you into divulging your bank account or credit card details.

CONCEPT OF ELECTRONIC FRAUD/3

TYPES OF ELECTRONIC FRAUD

AUCTION SITE FRAUD

- In regard to shopping and auction site fraud, innocent customers are robbed of their money by criminals through the exposure of their payment details in unsecure payment services.

- In most cases, online shoppers follow email links provided by criminals to enter into fraudulent sites, where they make payments without knowing.

CONCEPT OF ELECTRONIC FRAUD/4

TYPES OF ELECTRONIC FRAUD

PHISHING

- Phishing is a technique used to gain personal information for the purpose of identity theft. Phishing involves using a form of spam to fraudulently gain access to people's online banking details.

- As well as targeting online banking customers, phishing emails may target online auction sites or other online payment facilities.

- Typically, a phishing email will ask an online banking customer to follow a link in order to update personal bank account details.

CONCEPT OF ELECTRONIC FRAUD/5

TYPES OF ELECTRONIC FRAUD

CHARITY FRAUD

- The scammer poses as a charitable organization soliciting donations to help the victims of a natural disaster, terrorist attack regional conflict, or epidemic.

- Hurricane Katrina and the 2004 tsunami were popular targets of scammers perpetrating charity scams; other more timeless scam charities purport to be raising money for cancer, AIDS or Ebola virus research, children's orphanages (the scammer pretends to work for the orphanage or a non-profit associated with it), or impersonates charities such as the Red Cross.

CONCEPT OF ELECTRONIC FRAUD/6

TYPES OF ELECTRONIC FRAUD

ROMANCE SCAMS

- Dating and romance scams are some of the oldest in the book, but as long as people are looking for love, they won't be going away.

- Fraudsters may contact targets through phone, email, text, social media, or dating sites. They typically pose as a different person, including creating completely fake profiles (this is called catfishing), and often work in groups.

ACCOUNTANT AND ELECTRONIC FRAUD

- ✓ Whilst the majority of accountants are unlikely to ever be IT savvy enough to fully understand the intricacies of how cyber-attacks work, and be one step ahead of the hackers, they do have a duty of care to safeguard the digital assets and intellectual property of their own, as well as clients data. Failure to do this could result in reputational damage to the accountant and/or accounting firm, as well as potentially becoming implicated in such crimes.

- ✓ In terms of dealing with substantial gaps in cyber security levels, it is important to identify the most critical information assets, and get the basics right.

- ✓ For many organizations, this means dealing with fundamental security practices including boundary firewalls and internet gateways; secure configuration; access control; malware protection; and patch management. Basic discipline involves responding to new standards and regulation, understanding the weaknesses in legacy systems, and identifying where investment in technologies can help.

ACCOUNTANT AND ELECTRONIC FRAUD/2

Supporting smaller businesses is an important opportunity for firms to provide useful business advice. The professional accountant advisor can be particularly important in:

- Helping clients assess their governance and risk management - smaller businesses tend not to have strong risk management and control expertise. Accountants can ensure adequate business continuity and disaster recovery planning, particularly in the face of ransomware threats;

- Helping clients quantify risks and return on investment based on cost of breaches and stolen data and factors that impact cost; and

- Helping to mitigate risks with effective controls.

ACCOUNTANT BEST PRACTICES AGAINST E-FRAUD

It is unlikely that accountants will ever be one step ahead of the hackers, by following these steps they can severely limit the chances of themselves or their clients being victims of cyber attacks.

- **Initiating Different Passwords**

Assign different passwords to different pieces of software. This will limit the amount of accounts cyber criminals will be able to have access to. If all of your accounts have different passwords, and one of them has its security breached, this will limit the amount of data cyber criminals will have access to.

- **Change Passwords Regularly**

This will reduce the chance of hackers having access to accounts due to the likelihood of them having credentials which are out of date. Additionally, if you are the victim of a phishing attack you should change all of your passwords immediately.

- **Use anti-virus Be Cynical**

Question anything which looks unusual or suspicious. For example, be wary of clicking on links in emails requesting credentials, or responding to unusual email addresses requesting information..

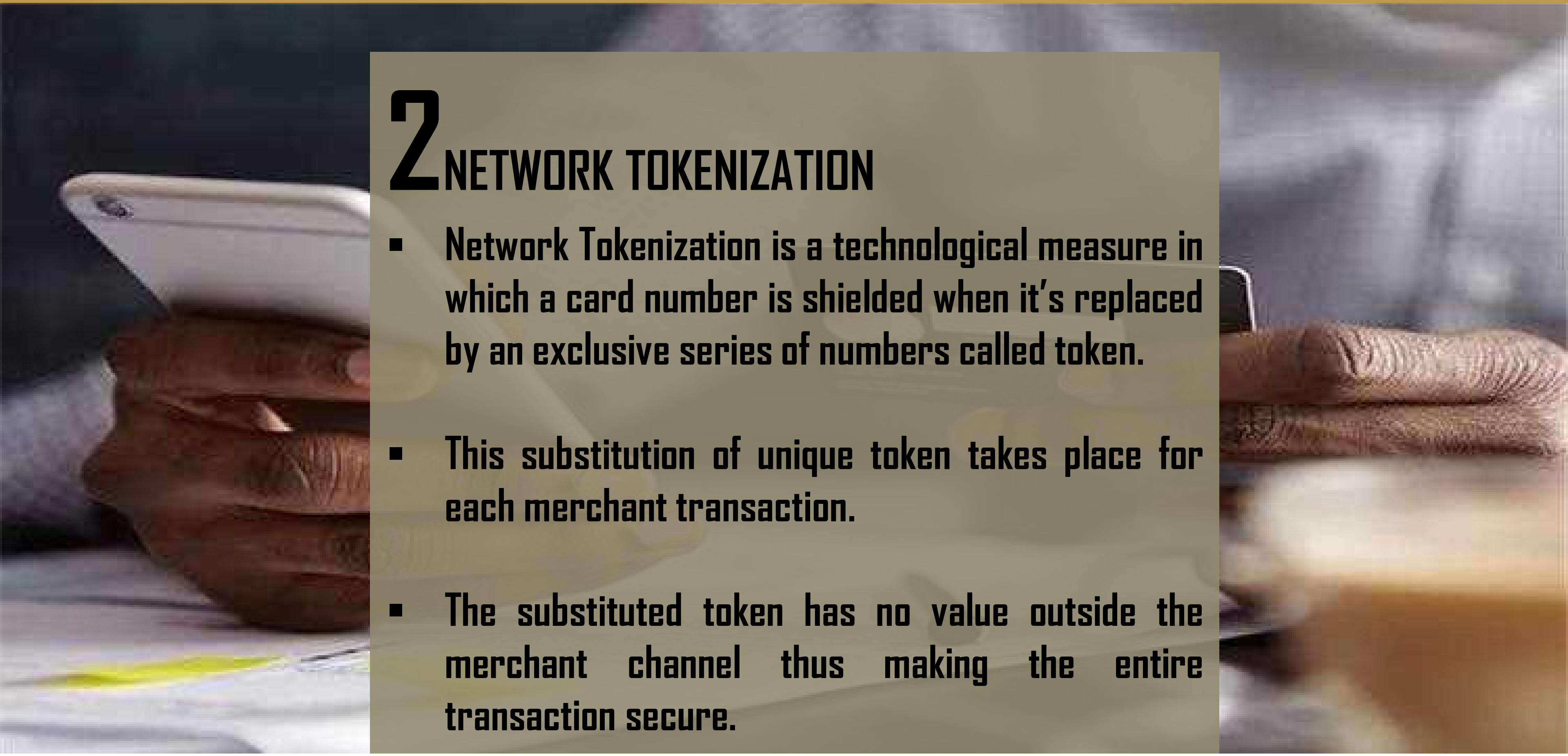
MEANS OF PREVENTING ELECTRONIC FRAUD

Electronic fraud is committed using communication platforms and can be control using the same medium.

1 ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING

- Transaction monitoring can be crucial in preventing digital payment frauds. With cutting edge technologies like AI and machine learning,
- one can identify fraudulent patterns in the history of transactions and then later apply them to check the authenticity of the current transactions.

MEANS OF PREVENTING ELECTRONIC FRAUD/2



2 NETWORK TOKENIZATION

- Network Tokenization is a technological measure in which a card number is shielded when it's replaced by an exclusive series of numbers called token.

- This substitution of unique token takes place for each merchant transaction.

- The substituted token has no value outside the merchant channel thus making the entire transaction secure.

MEANS OF PREVENTING ELECTRONIC FRAUD/3

3 BIOMETRIC AUTHENTICATION

- Biometric authentication has emerged as an effective way to eliminate digital payment frauds.

- Application of biometric authentication like finger, voice, eyes biometrics on the digital payment channels can easily identify fraudsters from that of legitimate users by recording and mapping pre-saved unique physiological characteristics.

MEANS OF PREVENTING ELECTRONIC FRAUD/4

4 BLOCKCHAIN

- Blockchain is another cutting-edge technology that can help in eliminating frauds in digital payments by augmentation of real-time transaction data sharing and by establishing an agreement of all parties.

MEANS OF PREVENTING ELECTRONIC FRAUD/5

5 ENCRYPTION

- Encryption is used in data communication to convert data on transit or stored to an indecipherable forms such that, the data will be meaningless to fraudster in the cause of interception.

- The policy here is that, it is only the owner of the message that can decrypt the data and make it meaningful. .

CHALLENGES IN CONTROL OF ELCTRONIC FRAUD

HUMAN RIGHTS IMPLICATIONS

- Human right struggle have place bounds or challenge most of the activities carried out for the purpose of identification.
- Human right has condemned the use of computer and networks in monitoring people, and maintain that the use of electronic in monitoring system and techniques on human bodies is tantamount to human right violation, abuse of privacy and abuse of power by authoritarian leaders who use their positions to humble their subjects and political opponents.

COMPLEXITY OF TECHNOLOGY

Technology is emerging continuously with different modus operandi. Some technologies relax certain restriction on users thereby making them anonymous. In such a situation, it becomes difficult to detect such criminal.

CONCLUSION AND RECOMMENDATION

- Conclusively, Electronic Frauds are the unwanted byproducts of digital payments which we must minimize and eliminate completely as soon as possible.
- Especially in this pandemic era where we all are dependent on digital payments, the space of digital payments must be made safe for all.
- To this end, government and financial Institutions should implement shielded authentication that is not vulnerable to spoofing of web.
- There is need for implementation of fingerprint authentication merged with graphical models that should include one-time authentication mechanisms which would be effective against both offline and online attacks from spoofing.
- In addition, accountant on the also also needs to heighten ethical awareness when it comes to considering what action to take when there has been a breach in either their own organization, or in one that they are advising.

CONCLUSION AND RECOMMENDATION/2

- ✓ Given the accountant's obligation to act in the public interest, it might be necessary to make a public disclosure, such as informing customers that their personal information has been exposed.
- ✓ If there has been a ransom demand, it might be necessary to seek specialist advice and support.
- ✓ On a final note, constant educational/ sensitization programs on electronic fraud need to be conducted to alert the users on how to always ensure a secured transaction on all electronic platforms.

PROFILE

Professor Godwin is a young but experienced multidisciplinary scholar-practitioner with over 25 years' experience and over 27 Professional qualifications from both Nigeria and International Professional Bodies. He is the co-founder and the Chief Technical consultant at OGE Professional Services Ltd, President at OGE Business School, Principal at Oyedokun Godwin Emmanuel and Co (Chartered Accountants, Forensic Auditor & Tax Practitioners).

Godwin is a professor of Forensic Accounting & Finance at Charisma University, Turks and Caicos Island, West indies UK., an Adjunct Professor in the Department of Management and Accounting of Lead City University Ibadan, Nigeria. He also currently lectures in the department of taxation, Nasarawa State University and McPherson University, all in Nigeria to mention few.

With years of Experience, Professor Godwin has held leading roles among notable firms such as Ibraheem Jimoh & Co Chartered Accountants, Saffron Professional Services, Chartered Institute of Taxation of Nigeria (CITN), Bond Group of Companies to mention a few.