European Journal of Business and Management
ISSN 2222-1905 (Paper) ISSN 2222-2839 (Online)
Vol.11, No.36, 2019

Investigating the Effects of Cyber Fraud on Customer Trust for Online Shopping: The Ghanaian Setting

Ming-yue FAN* Obrien NUNYUIE
School of Management, Jiangsu University, Zhenjiang 212013, China

Abstract
Cyber fraud has become a stumbling block in the development of many countries especially in the developing world as billions of dollars continues to be lost. It's prevalence in the west African sub-region has stifled the efforts made by governments to bridge the technology gap between nations like Ghana and the west. Online shopping which is a convenient advancement in technology and relatively famous form of transaction in the west requires a considerable level of trust between the customer and the service provider. With the consumer culture theory (CCT) and model of integrative trust as theoretical foundations, this paper adopts a comprehensive two-way generic inductive approach to gather relevant data for analysis to unravel the effects of cyber fraud on the Ghanaian consumers' trust for online shopping. The methodology encapsulates a systematic and rigorous literature review and documented cases of cyber fraud in Ghana. Results intimated that cyber fraud is a major cause of financial lose in Ghana and has to a large extent affected the Ghanaian consumers' trust for online shopping and E-transactions in general as only 39% of the populace are revealed to buy online. Poor information technology infrastructure, growth of IT users, and a lack of regulation and training law enforcements were also found to be the underlying causes of why it is challenging to secure information online and hence the lack of trust.
Keywords: Cyber Fraud, Trust, Online shopping.
DOI: 10.7176/EJBM/11-36-10
Publication date: December 31st 2019

1. Introduction

Fraud is a generic terminology and consists of multifarious ways by which people resort to get an upper hand or advantage over others mainly through tricks, surprises, false representation and any other methods of cheating (Singleton and Singleton,2010). To Wells (2010), fraud is an intentional falsification of statement aimed at financial gains from an innocent victim. Jegede (2014) retorts that, it is almost practically impossible to have a general laid down proposition to explain fraud. Having said this, it is critically important to state that cyber fraud, consumer trust, and online shopping are the main variables of interest to this paper: these terms have therefore been explained and lumped up in the following paragraphs to establish a logical relation between them.

This paper is focused on categories of fraud that is done via technology or through the internet: this is generally described as cyber fraud. Cyber fraud is birthed from modernization and globalization (Jegede,2014). According to the U.S department of justice, internet fraud is any form of fraud that use one or more components of the internet including emails, chat room, and websites among others to solicit financial gains from victims. The seriousness of Cyber fraud around the world has necessitated the need to find a long-lasting solution given the risks online business transactions are exposed to. Over the past years, many researchers have explored the relationships between the human environment, the rise in technology driven business transactions, growth of fraud and skepticism of attendants. For example (Kovarich,2008) posits that, global trade has steadily increased over the last century and is expected to increase even more rapidly as we mosey into a technologically intertwined world. In the same vein, Forrester research (2001) predicted a $1trillion worth of online goods and services purchases between 2001 and 2006 worldwide. This prediction did not only happen but also invariably raised concerns of the enormity of financial burden and risk factors that comes with doing E-business. This is what accounts for strict rules governing the conduct of business on the internet and why some consumers in different parts of the world remain skeptical about buying or doing business online. Consumer trust describes the extent to which a consumer believes that an organization is capable of protecting their personal data and also satisfying their demands. In 2017, the PWC conducted a research to understand what consumers think about data security, cybersecurity, trust, privacy and regulation. The study used online surveys and video interviews for 2000 American respondents who were over the age of 18. It is interesting to note that 69% of these respondents that companies are not doing enough to prevent hacks and cyberattacks which makes consumers trust organizations less. Only 25% of consumers in this research felt that companies have all it takes to protect their information with a relatively insignificant 10% believing they have absolute control over their personal data.

Quite contrastingly, the report gathers that consumers believe that businesses and not the government is better placed to protect them from internet fraud. Cyber fraud can be perpetrated usually if the criminals have some personal information of victims: this hinge again on consumer trust as the PWC (2017) report posits that 88% of respondents attribute their willingness to share personal information to trust and believe that the

information will be handled responsibly. Consumer trust is a serious issue which companies must make their topmost priority because trust for mainstream businesses is quite low.

An important observation from the above data is that banks and hospitals are trusted most even though there is online banking: this is probably attributable to long standing customer relationship or physical presence of bank anything consumer needs to have a face to face meeting. Marketing and online advertisements are the least trusted category. This could be because of cyber frauds start with an online advert.

On this basis, it can be intellectually assumed that once consumers build trust for a company, they become more willing to share information and hence transact business. This brings us to the third variable of importance, online shopping.

In the words of Petrovic, Ksela, Fallenbock, and Kittl (2003), "Online transactions and exchange relationships are not only characterized by uncertainty, but also by anonymity, lack of control and potential opportunism, making risk and trust crucial elements of e- commerce". Online shopping involves buying products online while eschewing the traditional methods of physically seeing, examining, and paying for a product. As stated by Petrovic et al (2003), online shopping breeds lots of uncertainties and before people go ahead to transact online, they must trust the company and be sure that there will not be any financial loses or deception of any form (cyber fraud).

Montague (2011) found that modes of payment for online transactions varied from one continent or country to the other. For example, Credit and debit cards are used more often while Europe, Africa, and Asia favor bank transfers and cash delivery. For an Asian country like China, this is no more the case as the Chinese society has become virtually cashless with E-commerce platforms like Taobao, J mall, and Pinduoduo being a necessary part of everyday life. In Essence, irrespective of the fact that there is internet or cyber fraud, there is trust for online shopping in China. The ITU (2008) postulates that unlike a decade ago, adoption and penetration of information and communication technology has significantly increased across the African continent and there has been a shift from dependence on cybercafes for internet access point to mobile access points through satellite connection and fiber optic cables in countries like Ghana, Nigeria, and Cameroon. Looking at Forrester (2011) prediction of 1 trillion dollars transaction worldwide, there is an indication that without taking appropriate measures cyber fraud will make a great deal of money for the perpetrators. It is in this light that Dutton, Helpser, and Gerber (2009) believe that fraud is on the increase and information on the seriousness of fraud often comes from government, research, insurance firms and of course fraud victims (Albrecht et al,2012). Now focusing on the financial losses caused by internet fraud, it is important to note that Germany loses over $40 billion a year (Fischer,2007) and in the U.S, about 7% of annual revenue is lost to fraud which was tantamount to some $994 billion. These figures are huge and disturbing as a major part of economic development is stifled by cyber fraud. A simple natural consequence of cyber fraud is probably lack of trust for online business transactions. In this vein, Longe et al., (2009) agree that, cyber fraud affects consumer confidence in online transactions. This is a clear indication that the internet is a double-edged sword: which means while providing opportunities for development, it increases information security risk (Magele,2005). Trust is very important in communicating especially when the environment is uncertain (Ma et al., 2009).

Ghana which is the country of interest to this paper was ranked among top 10 in cyber fraud activities in the world with Nigeria ranking 3rd according to the 2008 internet crime report. The bank of Ghana has clearly reported cyber-crime as the highest incidence of attempted fraud in the financial sector (Bank of Ghana,2017). Successive governments of Ghana have made efforts to build a knowledge-based economy hence making the Ghanaian economy ICT- driven. Internet usage in Ghana increased astronomically after the liberalization of the telecom industry in 1999. Online shopping is not very popular in Ghana as people prefer to see a product and check its quality before making physical cash payment. Also, it is hard for Ghanaians to easily trust that after paying for a product online (mainly through the famous mobile money platforms), their goods will still be sent. Not until the early 2010's, there was almost no form of online shopping in Ghana. Recent years have however seen the introduction of OLX and Tonaton online shopping platforms. Different factors can account for the lack of trust in E-buying in Ghana; some of these including culture, technological know-how and technology acceptance have been explored by other researchers but a link has not been established between cyber fraud which is very common and online trust. Is online buying behavior in Ghana really only about culture and uncertainty? What about the widespread cases of cyber fraud? Could cyber fraud victims be deterring others from shopping online by sharing their experience? The efforts put into this paper is therefore to assess how cyber fraud affects the trust Ghanaian consumers have for online shopping while outlining the various factors within cyber fraud that prompts doubt and mistrust. This study is significant in three folds: academic, social, and economic. Academically, it adds up to existing literature on online shopping, consumer trust, and cyber fraud but this time with unique focus on Ghana. Socially, it creates an awareness of how cyber-crimes are perpetrated in Ghana and some of the warning signs to look out for. This can significantly reduce how many people get defrauded on daily basis and hence leading to the economic relevance of saving money which could have been lost to fraud for development.

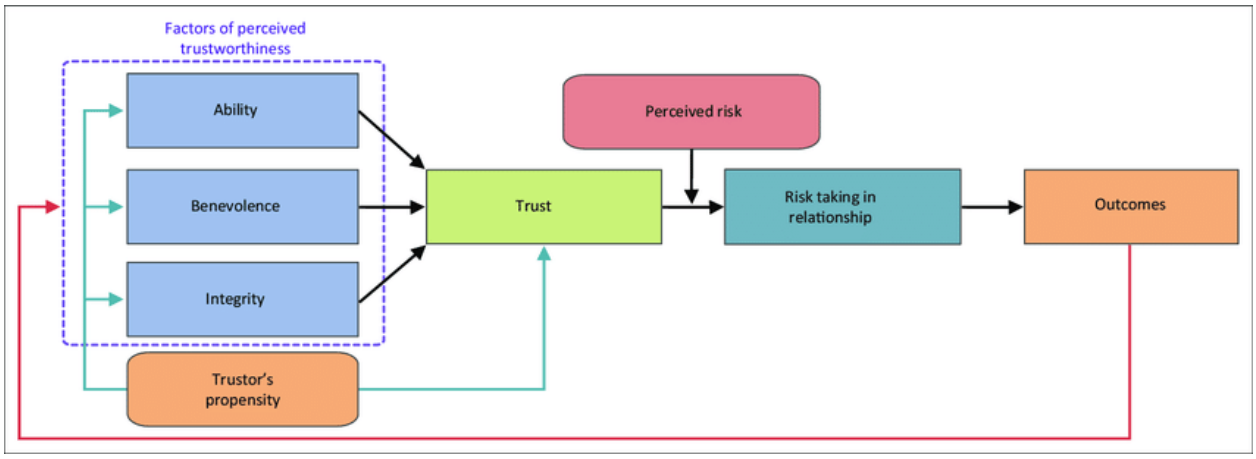
Literature Review, Methodology, and Results

2. Theoretical Foundations of the study

This section presents a chronological and logical analysis of literature on cyber fraud, shopping online, and of course trust on a global level. It Narrows further to discuss literature on the current situation of cyber fraud and its peculiar effects on consumers trust in Africa at large and more specifically Ghana. The section opens with the Model of integrative trust, consumer culture theory (CCT), conducts a simultaneous analysis of literature and their implication (results), and finally concludes with a conceptual model expansion.

2.1 Model of Integrative Trust

This model was proposed by Mayer et. al (1995) to explain the relational dimensions of trust. They define trust as "the willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control the other". Implicitly, trust checks how trustworthy a person is. This model views the formation of trust from the angle of two individuals in the context of any form of relationship. The rationale behind this model is that, trust is built through a continuous interaction and provision of information which is described as communication. Continuous interaction leading to trust will depend on the outcome of first interaction; a positive outcome builds trust and encourages further interactions but negative interactions kills trust. This model is suitable for this study because it seeks to unravel the thought processes a consumer goes through while communicating with an individual or organization in a bid to shop online and how trust is built ; hence in the context of this study and based on the model, trust could be built on the internet if two parties (consumer and online shop) viciously communicate and make information available to each other.



Source: Mayer et al (1995)

Figure 1. Integrative Model of interpersonal Trust

2.2 Consumer Culture Theory (CCT)

The concept of consumer culture theory explains the behaviors of consumers and choices they make from a socio-cultural point view rather than an economic or psychological one. In the words of Arnould and Thompson (2005), the CCT is not a unifying theory but "refers to a family of theoretical perspectives that address the dynamic relationships between consumer actions, the market place, and cultural meanings". The theory perceives culture as a numerous and fragmented construct and consequently a combination of different groups and shared meanings instead of a homogenous one (Firat and Venkatesh, 1995). Arnould (2006) defines consumer culture as a "social arrangement in which the relations between lived culture and social resources, between meaningful ways of symbolic and material resources on which they depend, are mediated through markets". The Consumer culture theory (CCT) is relevant to this study because it details how lived cultures and symbolic material resources influences the decision of a consumer to buy or transact business. Focusing on the setting of this study, consumers in Ghana have been used to the traditional way of shopping which requires physical presence and interaction for decades. Aside this, there were no major online trading platforms until the early 2010's. The introduction mobile money and online banking saw a massive acceptance by the Ghanaian populace nationwide but with regards to shopping from an anonymous seller online is problematic because of the longstanding traditional ways of shopping in Ghana.

3. Methodology

This paper adopts a comprehensive two-way approach to gather relevant data for analysis. The first part of the methodology is based on a systematic and rigorous literature review themed under definitions of trust, cyber

fraud, and online shopping, forms of cyber fraud, global challenges of handling cyber fraud, trust issues in shopping online, and existing theories explaining trust. The key areas of focus are on the methods used in these papers and their findings which provides a solid ground for critical analysis and conclusion. The second part of the method relies on data from documented cases of internet fraud in Ghana, how fraud is undertaken, and how the victims react to it; this gives insight into the forms of internet fraud that are mainly perpetrated in Ghana.

4. Results and Analysis

4.1 Definition of key terms: Cyber Fraud, Online Shopping, and Trust

Well (2010), defines fraud as an intentional falsification of statement aimed at financial gains from an innocent victim. Jegede (2014) retorts that, it is almost practically impossible to have a general laid down proposition to explain fraud. This paper is however focused on categories of fraud that is done via technology or through the internet: this generally described as cyber fraud. Cyber fraud in this paper refers to any form of crime committed in Ghana against a customer in the process of transacting business online by means of social engineering and trickery, Online Harassment, identity related crimes, hacking, and denial of service and information as taxonomized by Nurse (2017).

Many researchers have defined trust in variable ways: yet there is no single accepted definition of trust (McEvily et al.,2003) because it is a difficult to define concept with different facets (Fulmer and Gefand,2012; Castaldo et al,2010). Ebert (2009) categorizes interactive relationships that breed trust into: trust between individuals, organizations, and between a person and an organization. Various authors have shared their views on trust, some of which agree and disagree. Putnam (2000) views trust as a reciprocal concept which is developed through cooperation with others. In the view of Uslaner (2002), trust is not built based on cooperating or associating with others, but it is virtue (moral) that is learned from parents. This view is supported by Gillepsie et al., (2014) who also stressed that trust is not cooperation. A sharply contrasting view is brought up by Rothstein (2003) who looks at trust from the perspective of leadership. He opines that level of trust is a function of good governance. To Mayer et al., (1995), trust is "the willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control the other". Implicitly, trust checks how trustworthy a person is. Research on the variable and enormous definitions of trust indicates the prevalence of the common themes of behavioral intention and expectation (Bozic,2017). Based on the various definitions of trust, this study adopts and operationalizes the definition of Mayer et al., (1995).

Online shopping in this paper refers to the exchange of money for goods and services over the internet.

4.2 Forms of Cyber Fraud

Cyber fraud comes in variable and enormous ways which are devised by cybercriminals to exploit victims. The focus of this section is to highlight and typify the most significant and common types of cyber fraud that has been reported. Wall (2001) classified cybercrimes into crime against machines, crime against individuals, and crimes in the machine. Gordon and Ford (2006) also grouped cyber fraud into type 1 and type 2 cyber-crimes based on Wall's work. In this paper, the various forms of cyber fraud are taxonomized by Nurse (2018) to include social engineering and trickery, Online Harassment, identity related crimes, hacking, and denial of service and information. Nurse's taxonomy of cyber-crimes is focused on crimes against individuals which is of interest to the current study. Below is a detailed elucidation of these forms of cyber-crimes with diagrams to support.

To begin with, social engineering and trickery information implies using tricks to force people or an individual to behave in a certain way or perform a certain task. This kind of cyber-crime seeks to exploit individuals psychologically by using history and morals to manipulate them towards achieving a fraudulent goal. For example, a cyber-criminal can break into an individual's internet service provider account (Aktypi, Nurse, and Goldsmith,2017) by phoning the cell-phone providers help desk, pretending to be a spouse of the owner of the phone and using an audio of a crying baby to get sympathy from the help desk employee. At this point, requests can be made.

Online harassment explains situations in which an individual is tormented and abused by other online. It usually targets individuals with many inactions. Data and Research society (2016) found that, about 47% of internet users in the U.S have experienced online harassment at least once with a whopping 72% haven seen someone being harassed (Lenhard et al.,2016). This indicates the intensity of this problem and the need to address it.

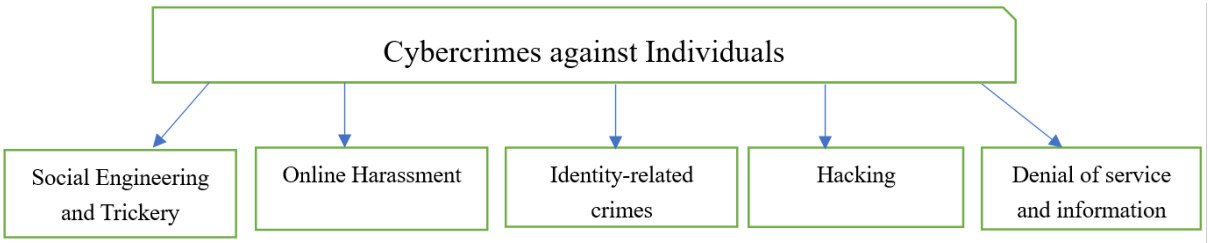
With identity related crimes, an individual's identity is used by others to undertake illegitimate activities or fraud. The identity of another person, usually a picture is used without his or her authorization. The amount of personal information kept online makes this type of cyber-crime easy. 173,000 identity fraud incidents were reported in 2016 in the U.K which translates into 53% of all fraud (on and offline) but more so contributed 88% of all online fraud (BBC,2017). Similarly, (Koops et al.,2009) intimates that identity fraud increased by 40% in

the U.S.

Hacking as a cyber-crime is very well known all over the world and has made frequent waves in news. It involves activities that has detrimental impacts on confidentiality of digital information or computer systems. Hacking in the corporate world simply refers to the exposure of personal data to third parties in an illegitimate way.

The final category is denial of service and information which is one of the most commonly used methods by cyber criminals. It simply means blocking access to information, websites, files and services.

Agyemang Duah and Asirifi (2015) gathered that the most prevalent form of cyber fraud in Ghana is deception which falls into the category of social engineering and trickery in the Nurse (2018) taxonomy and identity related crimes where a young man proposes to a rich lady online and extorts money from her. In subsequent sections, more elucidations are made on the forms of cyber fraud with evidence from key Ghanaian stakeholders and victims of fraud.



Source: Nurse (2018)

Figure 2. Taxonomy of Cybercrime

5. Challenges of Protecting internet-processed information from Cyber-Fraud

The revolution of information communication and technology has increased internet usage across the world and in effect increase online perpetrated crimes (Sarrab, Aldabbas, and Elbasir,2013). This has made it very important to secure internet-processed private and confidential information like government and military intelligence, banking information, and personal information. The problem however is that, securing the information is not easy as a result of many factors. Sarrab, Aldabbas, and Elbasir (2013) explored the challenges of information security in North Africa and found that just like all other African states, north Africa is challenged by information technology infrastructure, growth of IT users, and a lack of regulation and training law enforcements.

6. Trends of Online Shopping in Ghana

The 21st century presents a rather fast-moving and active world with human's speeding up their activities through the internet and computers: this is why it is called the 'computer age' (Chartterjee and Wang ,2011). This system has influenced businesses all over the world to move to the cyberspace hence the birth of e-commerce and e-banking among others which has given a new phase to methods of business transactions (Zakak,2000). Online shopping (B2C and B2B) has since grown at a great pace over the past decade and has therefore become practically impossible for businesses across the world to run with e-commerce of one form or the other (Sampeme,2015). Globally, online retail sales have grown at a rate of 17% since 2007 (A.T Kearny,2013) while Goldman Sachs projects an annual growth rate of 19.4% (Goldman Sachs,2015). In the same vein, Conlumino (2015) found that Africa and the middle east contributed 6% of the 13.76% global online sales increase rate in 2017. A.T Kearny (2013) projected global e-commerce sales to hit $1.92 trillion in 2016 and it went over the estimated figure by the end of the period. This is a great prospect for economic growth but e-commerce has been quite slow in developing countries (Nabareseh and Osakwe,2014) which can be attributed to the nature of the local environment, socio-economic and cultural factors, and poor infrastructure development (Boateng, Heeks, Hinson, and Molla,2008). It is further explained that, slow growth of e-commerce in Africa as compared to the west is a direct result of customer beliefs, values and rituals about how shopping should be done: these values and beliefs are birthed from their culture and therefore influences their thinking and approach towards technology use (Okoli and Mbarika,2003). Aside culture, technical know-how and ability to use technology also comes into play which is mostly seen as a result of limited infrastructure. E-commerce is very important and Jack Ma recounts that it controls about 5% of retail in China (YouTube,2015).

In Ghana, many individuals and firms are gradually joining the e-commerce wave just like in other countries (Agwu and Murray,2014) by using the internet as a platform to go global to create more opportunities and grow in revenue. Unfortunately, customers and internet service providers are not taking full advantage of the opportunities presented by online shopping (Sampeme,2015). The incorporation of e-commerce in Ghana has faced a myriad of challenges which stifles usage of its advanced forms after initial adoption (Boateng et al.,2014). Most e-commerce or online shopping practices in Ghana are generally limited to firms advertising products on

their websites and indicating their location for prospective customers to find them: a shift to the traditional system. It is rather shocking to note that irrespective of being ranked 49th in the world and 1st in Africa for broadband penetration coupled with a 71.5% literacy rate, increase in internet access, and ubiquitous use of high-tech gadgets, e-commerce and online shopping penetration is still lagging. Johnson (2015) also found that 100% of Ghana's population are familiar with the internet and use it frequently but unfortunately shopping online is notably low as only 39% buy online. Many researchers have focused on the role of consumers market place and culture, psychological, and technical barriers that stifles online shopping in a developing economy like Ghana. But in the wake of the 21st century, there is high literacy rate and widespread use of the internet for various purposes, yet there are limited studies about how internet or cyber fraud also slows down the development of online shopping. This brings in the dimension of trust which will be reviewed in subsequent sections. Why is it hard for Ghanaians to trust making transactions online? What effects does the widespread cybercrimes and attacks in Ghana have on this? What can be done to combat this menace of cyber fraud? This paper therefore seeks to fill these gaps in the literature relying on rigorous literature review and recommend ways for arresting the situation.

7. Trust and Online Shopping

Organizations have a technique relational asset if consumers trust them (Castaldo, Premazzi, and Zerbini,2010) since consumers provides a firm with the needed ingredients to operate functionally and financially well (Bozic,2017). In the past 10 years, several corruption scandals have hit top reputable organizations like Volkswagen and FIFA which according to Kim, Ferrin, Cooper, and Dirks (2004), damages consumer trust and leads to loss of competitive advantage by firms (Richard, Lawrence, and Burch,2011). In Ghana which is the focus of this paper, several scandals like the MENZGOLD and DKM scandals through which Ghanaians invested and lost millions of Cedis to what is described as a Ponzi scheme has made customer trust even lower (these were not even online transactions).

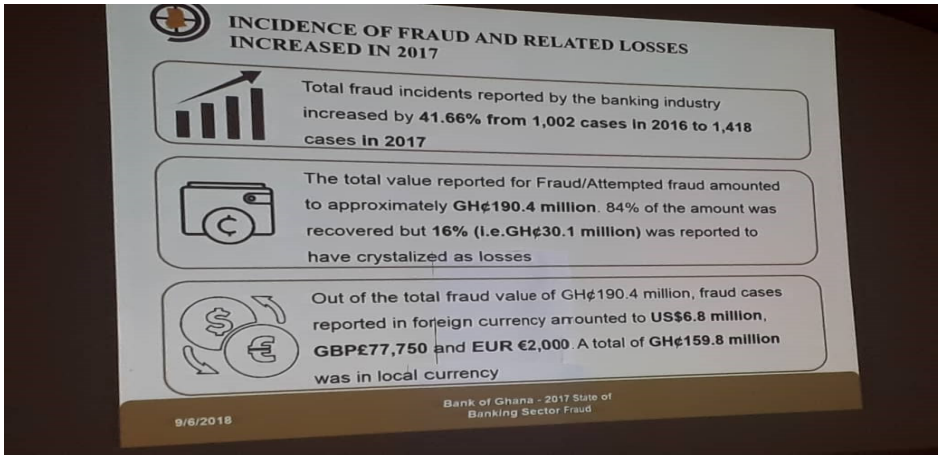
Assuming that e-commerce makes running a business easier, faster, and more effective is often flawed by perceptions of consumers about ethics of shopping online (Sampeme,2015). Some issues raised by consumers includes fulfilment, privacy and security, and non-deception on the internet since cyber criminals and hackers are on the look-out for victims: this is an important yet overlooked part of why online shopping is slow in Ghana. Roman and Cuestas (2008) posits that the extent to which an individual believes a site is safe for making financial transactions refers to security. Trust is an important aspect of utilizing any form of e-commerce or in this context, shopping online for growth and expansion (Roman,2007; Roman and Cuestas, 2008). It is important to state that, "trust" is different from "trustworthiness". Trust is generally the willingness to depend on another person in a risky situation (Serva et al.,2005) while trustworthiness emanates from the consumers from the consumers' willingness to make online transactions based on their perception of how credible the source is (Gefen and Straub,2003). The exposure of consumers to factors like dishonesty and deception which falls under the umbrella of cyber fraud affects their trust online (Murphy et al.,2005).

8. Cases of Internet Fraud in Ghana-Media reports, Police reports, Victims experiences and Bank of Ghana Alerts

This section focuses on cases of cyber fraud, the methods used by perpetrators, the extent of financial loss it has caused to the Ghanaian economy and what measures have been taken to curb the menace. Sources of information based the purposive sampling technique are from published information from newspapers, the criminal investigation department of the police, and other relevant reports presented on the issue viva-voce. This section establishes without any ambivalence that cyber fraud is a serious problem in Ghana.

8.1 Case 1

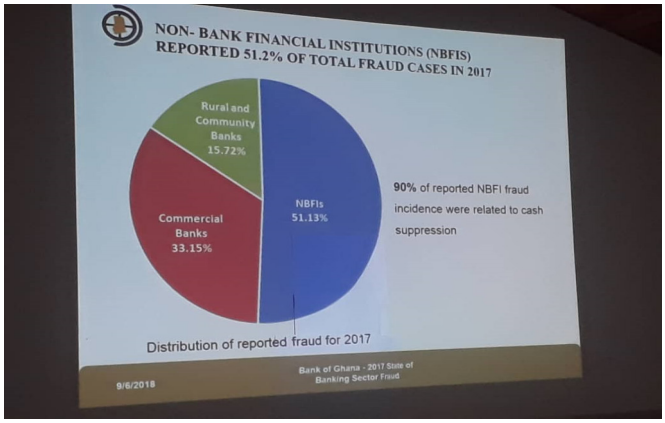
In the 2017, the bank of Ghana (BOG) presented a disturbing state of the banking sector fraud. This report intimates that between 2016 and 2017, cases of fraud in the banking sector has increased astronomically by 41.66%; that is from 1,002 cases in 2016 to 1,418 cases in 2017.



Source: Bank of Ghana (2017)

Figure 3. Fraud related losses in 2017

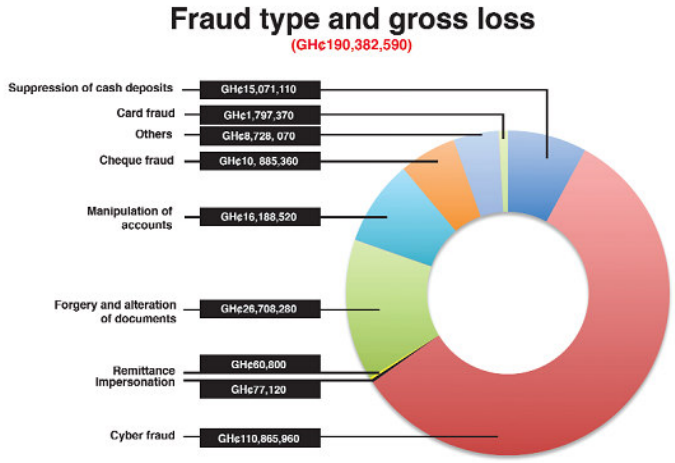
The above image from the report indicates the seriousness of fraud even in the banking sector which is supposed to be trusted. In 2017, GH ¢190.4 million is lost to fraud in the banking sector alone. The bank of Ghana also intimates at a seminar on cyber fraud in Senchi that internal staff in non-banking financial institutions (NBFI) were found to be responsible for 90% of cash suppression.



Source: Bank of Ghana (2017)

Figure 4. Financial Sector analysis of fraud distribution

It is critically important to state that non-bank financial institutions have the highest cases of fraud with cash suppression being the main method of perpetration. Now looking at the banking sector fraud trends in Ghana presented so far, it is clear that major policy steps must be taken to control the situation. An interesting dimension to the banking sector crisis however is that majority of attempted fraud happens via the internet. The bank of Ghana reports the threats of cyber fraud to the sector. By implication, a lot more money has been lost to cyber fraud than any other kind of fraud. At a financial crime sensitization program for banking industry stakeholders in Ada in 2017, Mrs. Akrofi, an advisor of the bank of Ghana notes that Ghana is among the top 10 most attacked countries through the internet: by implication, the advancement of the banking sector has significantly increased the attempts to defraud the sector. A research by the African union in collaboration with Symantec, a Ghanaian based IT firm in 2016 found that, 44 million spam incidents, 400,000 malware incidents, and 280,000 Bots incidents were recorded in Ghana. According to her, forms of fraud like card cloning, phishing, ransomware, and vishing shows how sophisticated the cyber criminals have become over the years. To curb this situation, Mrs. Akrofi stated that “the bank of Ghana in response to these lapses, has recently instituted a cyber security committee which have been mandated to implement the bank of Ghana’s cyber security directives”. The image below categorizes type of fraud and the financial loss caused.



Source: Bank of Ghana (2017)
Figure 5. Categories of fraud and financial lost caused

8.2 Case 2

On Tuesday, December 16, 2014, page 3 of the Daily Graphic, a famous newspaper in Ghana published a story on cyber fraud. It was captioned, "3 Nigerians busted for stealing Gh¢3 million through ATM Fraud". Ennin (2015), describes Ghana's economy as a high currency circulation economy as most transactions are done through cash. A consequence is that the central bank has to constantly print currency due to manhandling of currency notes by citizens. This is a very capital-intensive venture hence the option of online banking and transactions had to be considered: this is actually a brilliant way of cutting down the rate at which transactions are made with cash. A twist to this insight is that criminals have developed cloned ATM cards with which they make huge withdrawals from individuals account. A snapshot of the newspaper report relevant to this paper is quoted below.

"Three Nigerians believed to be members of a gang that manufactures and uses cloned Automated Teller Machine (ATM) cards to withdraw various sums of money from the accounts of a number of bank customers were arrested. Briefing the media, the Director of the Commercial Crime Unit of the Police Service, C/Supt of Police, Mr. Felix Mawusi said the suspects were arrested while they were in the process of withdrawing money from an ATM installation. He said members of the gang usually hang around ATM installations and offer to help card users who struggle to withdraw money from their accounts. Unknown to the card users, the suspects have devices such as phones that have been fixed with micro-cameras which they used to capture details on the card and the Personal Identification Number (PIN). The camera is fixed not to make any sound or flash while taking pictures. With the aid of their ATM manufacturing devices and electronic software applications, the gang then used the electronic code data they had captured to read and write the PIN on a cloned card. A total of ¢3million was siphoned by the gang. Police received a number of complaints from three banks that triggered the investigation which led to the arrest of the suspects".

Ghana is made up of several individuals who run their private business on a sole proprietor basis. Most of these people are petty traders whose businesses are classified under small medium enterprises (SME's). As the central bank works on making the economy cashless, miscreants like the case above keep scaring people from engaging in online transactions there by deepening the traditional methods of using cash and meeting personally to buy or pay for goods and services.

8.3 Case 3

Another case of cyber-fraud was reported 'the Ghanaian times' (a credible newspaper in Ghana) on the 27th of January, 2015, page 3: this report was captioned "6 Busted over Sim Box Fraud". For a government to be able to provide adequate services and infrastructure for its citizens, it needs funding. Most governments consider tax as an important source of revenue to develop their countries. Parliament (Ghana's law-making body) passed the communications service Act (754) in 2008 purposely to gain additional revenues from the services telecom companies provide to customers. The problem now is that "sim box" fraudsters are diverting calls via the internet hence cutting short millions of Ghana Cedis in revenue which could go a long way to boost the economic growth of the country. Sim box fraud as reported by "the Ghanaian times" is very technical and hard to deal with. The newspaper report is as follows;

''Six people, including Dr. Alex Tweneboah, former president of the Ghana Real Estate Developers

Association (GREDA) and lecturer at the Asheshi University were in police custody. The other five arrested in separate operations in Kumasi, Tema, Accra and Koforidua by task force made up of detectives from the CID Headquarters, Officials from the National Communications Authority and various telecom operators, with technical assistance from SUBAH Info Solution, Ghana Limited. More than 21, 000 assorted SIM cards of the various mobile networks, laptops, printers, internet modems and heavy-duty batteries were found with them. The Director-General of CID, Mr. Agblor explained that SIM box "fraud occurs when individuals or organizations illegally terminate a voice call which is the preserve of registered licensed network operators and usually at lower costs than approved rates". Fraudsters then used to channel the national calls away from licensed international gateway operators and presented as local calls on unlicensed networks. The suspects were arraigned on two counts of illegal termination and operation of telecommunications without authority under the Electronic Transaction Act, 2008 (Act 772). Briefing the journalists on the successful operations by the task force, the Minister of Communications, Dr Omene Boamah hinted that the activities of SIM box fraud have cost the nation $33,592,320 or GH¢107,459,000 in revenue loss between July 2014 and early January, 2015. He added that the amount involved was worrying and urged the telecommunications operators to strengthen their software to detect unregistered SIM card in the system''.

The above report shows how people with high social ilk like professors and directors hide behind the guise of the internet to misconduct themselves. If those with authority and influence are joining the perpetrators of cyber-crime, it will be really challenging to deal with this menace.

8.4 Case 4

With surge of the internet in our world today, people in different parts of the world are able to communicate with each other on real time basis and transmit information instantly through social media platforms like Facebook, Instagram, Imo, WhatsApp, Telegram, WeChat, and twitter among others (Enin,2015). The world wide web (www) makes this interconnection very convenient. A negative twist to the overwhelming benefits of the internet is sexual harassment. The internet has given the opportunity to some unscrupulous individuals to target children and minors with their insatiable sexual fantasies. The form of fraud via the internet falls perfectly in the sexual harassment category of the Nurse (2018) taxonomy of types of fraud perpetrated against individuals. Sexual harassment on the internet is not only prevalent in Africa and the developing world, it is a global canker. On the 24th of October 2015, 'The Daily Graphic' (a highly reputable newspaper) captured a case of adolescent internet sex crime and this shows how diverse and dynamic cyber-crime is in Ghana. The narrative captured the 'Daily Graphic' is elucidated below.

*"**Dr. Ali-Gabass, a gynecologist at the Effia Nkwanta Hospital in Sekondi, was said to have had a canal knowledge of his victim five times at Kasoa in the Central Region and Alajo in Accra between October 2013 and April 2014. The victim after fifth incident, started experiencing excruciating pains and the parents rushed him to Kole Bu Teaching Hospital for treatment. While receiving treatment at the facility, the victim was diagnosed with HIV and he mentioned Dr. Ali-Gabass as the one responsible for his complications. The police prosecutor charged the accused on two counts of defilement and unnatural canal knowledge. According to facts of the case, the victim had encountered with the accused on Facebook and they became friends. They had a chat online and communicated by phone for a while until in October, 2013 when the accused arranged and met the victim at Kosoa where he forcibly had anal sex with him in his car. Subsequently, Dr. Gabass was found guilty and sentenced to 25 years" imprisonment"** (Daily Graphic, 14th July, 2015:3).*

This incidence is absolutely unacceptable and shows that parents are usually negligent of their kids' usage of social media and this increases the risk of victimization (Marcus,2008).

9. The Effects of Cyber Fraud on the Ghanaian Consumers Trust for Online Shopping

Analyzing the current trends of shopping online in Ghana as shown in earlier paragraphs reveals a ridiculously low patronage. This in my discretion is not only as a result of culture but also the explosion of cyber fraud cases in the country. Traditionally, Ghanaians prefer to be physically present and interact with a seller before making a decision of buying a product. However, the rise of technology has brought on board the phenomenon of shopping online whose modus operandi already deviates from the norms of shopping in Ghana. The populace could have gone through the process of technology acceptance by perceiving the ease of use and its usefulness to life; this process was however slowed down by the issues of fraud online hence deepening the need to remain traditional. Johnson (2015) found that 100% of Ghana's population are familiar with the internet as use it frequently but unfortunately shopping online notably low as only 39% buy online. Most e-commerce or online shopping practices in Ghana is generally limited to firms advertising products on their websites and indicating their location for prospective customers to find them: a shift to the traditional system. It is rather shocking to note that irrespective of being ranked 49th in the world and 1st in Africa for broadband penetration (9) coupled with a 71.5% literacy rate, increase in internet access, and ubiquitous use of high-tech gadgets, e-commerce and

online shopping penetration is still lagging. The reviewed cases of fraud and warning from the Bank of Ghana and police department has created great awareness on the need to be careful while making and form of online transactions but has also broken the trust Ghanaians have for buying online.

10. Conclusion

Cyber fraud is a real menace and in Ghana, the most prevalent forms are deception and trickery, identity fraud, and sim box fraud. The country loses billions of dollars annually to fraud perpetrated online alone hence, authorities have taken appropriate measures to track and arrest criminals. Public awareness has also been created to conscientize the Ghanaians on the risks involved while they surf the internet to make transactions. These were steps in the right direction but has unfortunately created negative perceptions about shopping online. Going forward, it is laudable for the government the tackle the challenges of cyber security like poor information technology infrastructure, growth of IT users, and a lack of regulation and training law enforcements. The lack of trust for the online systems in Ghana is birthed from the challenges of securing information online. If these systems are better placed, the people will develop confidence in using convenient online methods to buy and sell. This would go a long way to bridge the information technology gap the Ghanaian government seeks to bridge. For future research more attention can be placed on technology acceptance and the psychology of the consumer and how that can improve the rate of online transactions and shopping activities. If appropriate measures are put in place to boost the Ghanaian consumers' trust for online shopping, there will be a positive impact on economic growth and will better connect the country with the rest of the world in international trade. It must however be emphatically stated that, cyber fraud will continue to be a necessary evil and a threat as far as we shop online. The threats can only be reduced to the barest minimum but not absolutely eradicated as cyber criminals continue to adopt new strategies with the rise of technology.

References

Agwu, M. & Murray, P., 2014. Drivers and Inhibitors to e-Commerce adoption among SMEs in Nigeria. *Journal of Emerging Trends in Computing and Information Sciences,* 5(3), pp. 192-199.

Aktypi, A., Nurse, J. & Goldsmith, M., 2017. *Unwinding Ariadne's Identity Thread: Privacy Risks with Fitness Trackers and Online Social Networks. In: Proceedings of the 2017 International Workshop on Multimedia Privacy and Security.* ACM,New York, USA, CCS Computer and Communications Security.

Albrecht, W. S., Albrecht, C., Albrecht, C. & Zimbelman, M., 2012. *Fraud Examination.* 4th ed. Mason, OH South Western: Cengage Learning.

Arnould, E., 2006. Global Consumer Culture. *Encyclopedia of International Marketing.*

Arnould, J. & Thompson, C., 2005. Consumer Culture Theory (CCT): Twenty Years of Research. *Journal of Consumer Research,* 31(4), pp. 868-882.

AT. Kearny, R., n.d. Global Retail Ecommerce Index. pp. 1-7.

Boateng, H., Hinson, R., Heeks, R. & Molla, A., 2008. E-commerce in Least Developing Countries: Summary Evidence and Implications. *Journal of African Business,* Volume 9, pp. 257-285.

Boateng, R., Olumide, L., Isabalija, R. & Budu, J., 2011. Sakawa-Cybercrime and Criminality in Ghana. *Journal of Information Technology Impact,* 11(2), pp. 85-100.

Bozic, B., 2017. Consumer Trust Repair: A Critical Literature Review. *European Management Journal,* pp. 1-10.

Castaldo, S., Perrini, F., Misiani, N. & Tencati, A., 2009. The Missing Link between Corporate Social Responsibility and Consumer Trust: The Cae of Fa& Trade Products. *Journal of Business Ethics,* Volume 84, pp. 1-14.

Castaldo, S., Premazzi, K. & Zerbini, F., 2010. The Meanings of Trust. A Content Analysis on the Diverse Conceptualizations. *Journal of Business Ethics.*

Chatterjee, P. & Wang, Y., 2011. Online Comparison Shopping Behavior of Travel Consumers. *Journal of Quality Assurance in Hospitality and Tourism,* 13(1).

Duah, F. & Asirifi, M., 2015. The Impact of Cyber Crime on the Development of Electronic Business in Ghana. *European Journal of Business and Social Sciences,* 4(1), pp. 22-34.

Dutton, W., Helpser, E. & Gerber, M., 2009. *The Internet in Britain: 2009 OxlS Report.* Oxford Internet Institute: University of Oxford.

Ebert, T., 2009. Facets of Trust in Relationships- A Literature Synthesis of Highly Ranked Trust Articles. *Journal of Business Market Management,* 3(1), pp. 65-84.

Firat, F. & Venkatesh, A., 1995. Marketing in a Postmoden World. *European Journal of Marketing,* 29(1), pp. 40-56.

Fischer, 2007. *DicZeit04.01.2007.* [Online] Available at: http://newsbbc.co.uk/english/static/indepth/uk.2001/lifeofcrime/cybercrimes [Accessed 10 November 2019].

Forrester-Research, 2012. *Forrester Research.* [Online]

Available at: http://www.oscwork.com,au/231/-Australia-Ecommerce-Statistics.html [Accessed 18 November 2019].

Fulmer, A. & Gelfand, M., 2012. At What Level (and in whom) we Trust Across Multiple Organizational Levels. *Journal Management,* Volume 38, pp. 1167-1230.

Gefen, D. & Straub, D., 2003. Managing user Trust in B2C e-services. *E-services Journal,* 2(2), pp. 7-24.

Gelepsie, N., Dietz, G. & Lockey, S., 2014. Organizational reintegration and trust repair after an integrity violation: a case study. *Business Ethics,* 24(3), pp. 371-410.

Gordon, S. & Ford, R., 2006. On the Definition and Classification of Cybercrime. *Computer Virology,* 2(1), pp. 13-20.

Jegede, A., 2014. Cyber Fraud, Global Trade and Youth Crime Burden: Nigerian Experience. *Afro Asian Journal of Social Sciences,* V(Quarter IV), pp. 229-5313.

Johnson, G. W., 2015. An Investigation into the online purchasing behavior of university students in Accra. *Ashesi Institutional Repository.*

Kim, P., Ferin, D., Cooper, C. & Dirks, K. T., 2004. Removing the Shadow of Suspicion: The Effects of Apology Versus Denial for Repairing Competence- Versus Integrity-Based Trust Violations. *Journal of Applied Psychology,* 89(1), pp. 104-18.

Koops, B., 2010. The Internet and itd Opportunities for Crime. In: *Herzog-Evans, M(ed) Transitional Criminology Manual.* Nijmgen, Netherlands: WLP, pp. 735-754.

Lenhard, F. et al., 2016. "On My Own, but Not Alone"-Adolescents' Experiences of Internet- Delivered Cognitive Behavior Therapy for Obsessive compulsive Disorder. *PLoS ONE,* 11(10).

Longe, O., Ngwa, O., Wada, F. & Mbarika, V., 2009. Criminal Uses of Information and Communication Technologies in Sub-Saharan Africa: Trends, concerns, and Perspectives. *Journal of Information Technology Impact,* 9(3), pp. 155-172.

Magele, T., 2005. E- security in South Africa. *White Paper prepared for the ForgeAhead e-Security event.*

Mayer, C., Davis, J. & Schoorman, F., 1995. An Integrative Model of Organizational Trust. *The Academy of Management Review,* 20(3), pp. 709-734.

McEvily, B., Perrone, V. & Zaheer, A., 2003. Trust as an Organizing Principle. *Organization Science,* 14(1), pp. 91-103.

Montague, D., 2011. *Essentials of Online Payment Security and Fraud Prevention.* 3rd ed. Hoboken, N.J: John Wiley & Sons,Inc.

Murphy, P., Laczniak, G., Bowie, N. & Klein, T., 2005. *Ethical Marketing.* Upper Saddle River,NJ: Pearson.

Nabareseh, S. & Osakwe, N., 2014. A Comparative Study of Consumers' Readiness for internet Shopping in Two African Emerging Economies: Some Preliminary Findings. *Mediterranean Journal of Social Sciences,* 5(23), p. 1882.

Nurse, J., 2018. Cybercrime and You: How Criminals Attack and the Human Factors that they seek to exploit. In: *The Oxford Handbook of Cyberpsychology.* Kent: Oxford University Press.

Okoli, C. & Mbarika, V., 2003. Assessing E-Commerce in Sub-Saharan Africa. *Journal of Global Information Technology,* Volume 6, pp. 44-66.

Petrovic, O., Ksela, M., Fallenbock, M. & Kittl, C., 2003. Trust in the Network Economy. *Springer,* Volume 2.

Putnam, R. D., 2000. *Bowling Alone-The collapse and Revival of American Community.* 1st ed. New York: Simon & Schuster Paperbacks.

Richards, C., Lawerence, G. & Burch, D., 2011. Supermarkets and Agro-industrial Foods. *Food Culture and society,* 14(1), pp. 29-47.

Roman, S., 2007. The Ethics of online Retailing: A scale development and Validation of customers' perspective. *Journal of Business Ethics,* 58(4), pp. 439-445.

Roman, S. & Cuestas, P. J. D., 2008. The Perceptions of Consumers Regarding Online Retailers' General Internet expertise and word of mouth: A preliminary Analysis. *Journal of Business Ethics,* 83(4), pp. 641-656.

Rothstein, B., 2003. Social Capital, Economic Growth and Quality of Government: The causal mechanism. *New Political Economy,* 14(1), pp. 67-87.

Sarrab, M., Aldabbas, H. & Elbasir, M., 2013. Challenges of Computer Crime Investigation In North Africa's Countries. *International Arab Conference on Information Technology (ACIT'2013).*

Serva, M., Benamati, J. & Fuller, M. .., 2005. Trustworthiness in B2C E-Commerce: An Examination of alternative Models. *The Database for Advances in information Systems,* 36(3).

Singleton, T. & Singleton, A., 2010. *Fraud Auditing and Forensic Accounting.* 4th ed. New Jersey: John Wiley & Sons .

Uslaner, E., 2002. *The Moral Foundations of Trust.* New York: Cambridge University Press.

Wall, D., 2001. *Crime and the Internet.* London: Routledge.

Well, J., 2010. *Internet Fraud Casebook: The World Wide Web of Deceit,Hoboken.* New Jersey: Wiley and Sons Inc.