European Journal of Business and Social Sciences, Vol. 4, No. 01, **April 2015.** **P.P. 22 – 34**
URL: *http://www.ejbss.com/recent.aspx-/*
ISSN: 2235 -767X

THE IMPACT OF CYBER CRIME ON THE DEVELOPMENT OF ELECTRONIC BUSINESS IN GHANA

Frank Agyemang Duah

Department of marketing
Takoradi polytechnic Box 256 Takoradi W/A
Corresponding author: fagyemangd@yahoo.com
Tel: +233-203322475

Asirifi Michael Kwabena

Department of mathematics and statistics
Takoradi Polytecnic Box 256
asirifimk@yahoo.com

ABSTRACT

The identification of Information and Communication Technology (ICT) as an essential tool for sustainable development has proved to be worth every investment. As a result of this, Internet usage in Ghana has grown rapidly resulting in the explosion of Internet Service Providers (ISPs) and Internet access points. This has had several positive impacts on the socio-economic and educational developments in the country. Unfortunately, the country's image has also suffered as a result of the nefarious activities of some Ghanaians that have now turned the Internet into a cheap channel for the perpetration of crime. This study is therefore directed towards understanding the extent of fraudulent cyber activities and its impact on the development of electronic business in Ghana. A secondary data was analysed by the use of generic inductive approach. Results indicated that cyber fraud is fast gaining grounds in Ghana and it cause direct financial losses to consumers and businesses
*Keywords**: cyber-crime, sakawa, Electronic business, ICT.***

1. Introduction

As online crime has grown more prevalent, consumer confidence has plummeted. Unlike the old days when hackers created viruses to be mischievous, modern-day malware authors create threats primarily to make profit. As the "Underground Economy" has grown and flourished, cyber criminals have developed new methods for tricking victims into downloading Trojans. These scams are amazingly lucrative, with profits totalling in the millions per year. Many perpetrators hail from Eastern Europe where cybercrime is rampant and considered business as usual.

According to the 2008 Internet Crime Report, published by the Internet Crime Complaint Centre (IC3), from January 1, 2008 through December 31, 2008, 275,284 complaints were filed online with IC3. This figure represents a 33.1 percent increase compared to 2007 when 206,884 complaints were received

A new study by Norton reveals the staggering prevalence of cybercrime: 65% of internet users globally, and 73% of U.S. Web surfers have fallen victims to cyber crimes, including computer viruses, online credit card fraud and identity theft. As the most victimized nations, America ranks third, after China (83%) and Brazil and India (76%).

According to the International Telecommunication Union, Internet users in Ghana reached 1,297,000 as of June 2010 representing 5.3% of Ghana's population. The internet is the driving force for growth of e-business. Ghana's growth potential is limited by the lack of infrastructure (connectivity) and equipment. The Government of Ghana is making concerted efforts to create a 'knowledge-based economy' thereby making Ghana an ICT – driven economy. The Government of Ghana in 2006 launched the national fiber-optic backbone project to enhance internet connectivity throughout the country. The objective of this project was to provide a reliable and cost effective access to broadband connectivity nationwide to improve the use of ICT in the country and also enhance e-business.

Over the last few years, the evaluation of the internet has evolved from being scientific to a platform that is enabling a new generation of businesses. E-business is a relatively new and fast paced approach to meeting consumer needs, introducing new products, and spanning geographic boundaries such as oceans and mountains. E-business growth worldwide reached US$2.5 trillion in 2009 being that years' total value of e-business transactions worldwide.

While there are many positive aspects of this new e- business model, e-crime has become a serious concern for all e-businesses, with a significant impact on the bottom line. We conceptualize cybercrime as criminal activities or crimes in which computing devices or other forms of ICTs are the target (Pati, 2003). From the perspective of ICT for development, it is not misplaced to say that cybercrime portends some dangers and has the potential to stall the developmental contributions accruable from a well-harnessed ICT adoption, diffusion and usage in Ghana. The Internet, by its very design, is an inherently vulnerable network which has enabled cyber crime to flourish in a new virtual 'Wild West' environment.

Cyber fraud has a potential to widen the digital divide, crumble the information infrastructure and affect consumer confidence in online transactions (Salifu, 2008; Longe, O., Ngwa, O., Wada, F., Mbarika, V. and Kvasny, L. (2009); Oumarou, 2007). E-businesses face many challenges, especially in today's turbulent economy, and the effects of cyber fraud make it even harder for the business to be profitable and survive. Therefore, the nub of this study is to identify the various cyber fraud schemes and the extent to which they affect the e-business sector in Ghana.

1.1. *The Upsurge of Cyber Crime 'Sakawa' In Ghana*

The use of the Internet in Ghana has seen a significant increase since the liberalization of the telecommunication industry in the 1990's. The country had 43 Internet users per 1,000 people in 2008 as compared to 1 Internet user in 1999 (ITU, 2009). The number of PC ownership doubled to 52 owners per 1,000 people between 1999 and 2005 (ITU, 2007). With these developments also comes negative effects and unintended consequences of ICT, particularly, cyber-crime.

"Sakawa" is a Hausa term that consists of the root 'saka-' [to put it in] and 'wa' (a simultaneously past and plural affix). Combined, these affixes literally mean 'to [have] put something in. 'Sakawa' is a coinage by youth fraudsters from deprived communities in Accra such as Nima, Mamobi and Lagos Town. The word indexes an 'azaa' (fraudulent) activity where cyber fraudsters' alleged involvement in occultism rituals is aimed to compel their victims to accede to their demands. These alleged rituals include taking an oath not to divulge 'sakawa' secrets and to fully abide by 'sakawa' rules; inflicting wounds that never heals; sleeping in coffins for specified days at cemeteries (maximum being a week); carrying coffins in the dead of the night at road-intersections while being semi-naked; drinking human blood obtained either from murdering someone or from discarded female menstrual pads; eating contents from rubbish dumps for a required number of days; abstaining from bath before and after making a hit (In sakawa lingua culture, a 'hit' principally refers to a successful receipt of funds transferred through money transfer process like Western Union or Money Gram as well as other material items.); spiritually sacrificing one's manhood (which manifests either as impotence or not being able to have children .

In terms of the strategies that these fraudsters allegedly use, therefore, a plethora of these two will be discussed for illustrative purposes.

In this type, the perpetrator manages to contact the victims either through mass-mailing or through a lead. The victim is promised an incredibly profitable return on his investment (usually shady and dubious). The popular baits include gold, diamond, lottery and some abandoned money that the client can help recover.

Whatever, the bait, the true bait is the promise of instant wealth for the victim. These are well crafted plans with alibis that those who use fake documents sometimes originate from genuine sources such as the Office of the President, Attorney General's Department and respectable banks. At times a duplicate website is designed which may look similar to a legitimate one or will redirect to a legitimate one when visited. Whatever be the case, the success of this modus operandi is basically ignorance or greed on the part of the victim. In the worst case scenario, the victim is lured to a location and physically attacked and robbed… or even killed. It is believed that this type of cyber fraud was carried over with the influx of Nigerians into Ghana. However, it has seen a sturdy decline since 2006. The returns from this activity can range from 1,000 to 1,000,000 dollars.

After creating an online profile, a sakawa person will send baiting emails which establish the basis for an initial friendship if the 'mugu' (client or the targeted person) responds. The fraudsters use this stage to profile and assess the generosity or seriousness of the client. Testing this characteristic involves requesting items like cologne, lingerie, explicit or near explicit pictures of the client. If this is accomplished, then the stage is set to demand bigger sums of money.

In the other type, the perpetrator is usually a young man posing as a woman (90%) or a young woman posing as a grown woman (7%). The remaining 3% are gay. Often these perpetrators are poor and hungry with no real options for making ends meet or a real career path.

Here, these fraudsters scout dating sites and examine profiles of males/females who are interested in relationships. They would then create profiles that match those of their potential 'mugu' (client). Here they use photographs either taken from the web or that of a female accomplice. The victim is usually a bored rich old man or someone in the mid-forties. The perpetrators present themselves as a fabulously luscious young lady (using pictures from pornographic or fashion websites). The promise of overseas love is found so attractive and irresistible that the victim (who at times is a dissatisfied husband or wife or attention deprived) will do anything to get this kind of attention. The victim commits to love over the internet with the hope that they will meet their lovers eventually.

1.2. *Cyber-Specific Laws*

Cyber specific laws fall into three categories; enabling, prohibition and investigation. Enabling typically gives legal effect to electronic documents and storage. For example, digital signatures can legally work as real signatures only when legislation provides such judicial capability. Evidence for tax or other purposes can be effective when a specific law defines electronic exchange and storage to be sufficient as evidence.

Prohibition typically barns and punishes computer related crimes. In Ghana, electronic data destruction cannot be criminalized under the general law, because it does not destroy any physical matter. Similarly, intrusion itself does not constitute a crime as it does no physical harm. Thus, a specific law is required. Unauthorized Access Prohibition act is therefore required in Ghana to cater for this.

For investigation purposes Internet Service Providers are typically required to reserve communication logs for a certain period of time and submit such records to national investigative agencies. As communication service providers are prohibited from divulging communications secrets, specific legislation is required to give exemption. Eavesdropping and network monitoring for specific communication also should be allowed under a jury court's order judged in line with a law allowing special investigation. These types of laws are prepared to indirectly fight against threats.

2.0. Method

2.1. *Research Design and Instrumentation*

A secondary data analysis approach was adopted for the study. Data for this research and analysis was taken from the internet, books and papers published by other authors and researchers in areas related to the research topic.

Data was also collected from newspaper articles and news articles from various online news outlets.

The research presented in this article is a summation of the data collected from the sources over a six month period. Most of the articles used span from 2000 to 2011 and are thus still relevant.

A generic inductive approach for data analysis was used, as suggested by Thomas (2003). The approach is not only convenient but also efficient in analyzing qualitative data and the quality of the conclusion derived from this analysis is in no way lower than the conclusion drawn from the above mentioned specific traditional approaches(Thomas, 2003). Moreover, the approach is based on the pattern derived from the analytical techniques usually used in qualitative studies. The three purposes of using this approach in the analysis, as described by Thomas (2003), are in line with the aim and objective of the present study. These purposes were:

- To condense extensive and varied raw text data into a brief, summary format.
- To establish clear links between the research objectives and the summary findings derived from raw data.
- To develop model or theory about the underlying structure of experience or processes which are evident in the raw data.

It tries to analyze the collected data through multiple reading and interpretation to answer the research questions. After this primary analysis, categories were derived from the raw data which were used as key themes. The researcher then made decision about the important and less important themes on the basis of the dominance of the themes in the secondary data and on the basis of the information obtained from the literature review.

3.0. **Results and Discussion**

3.1 *E-Fraud in Ghana*

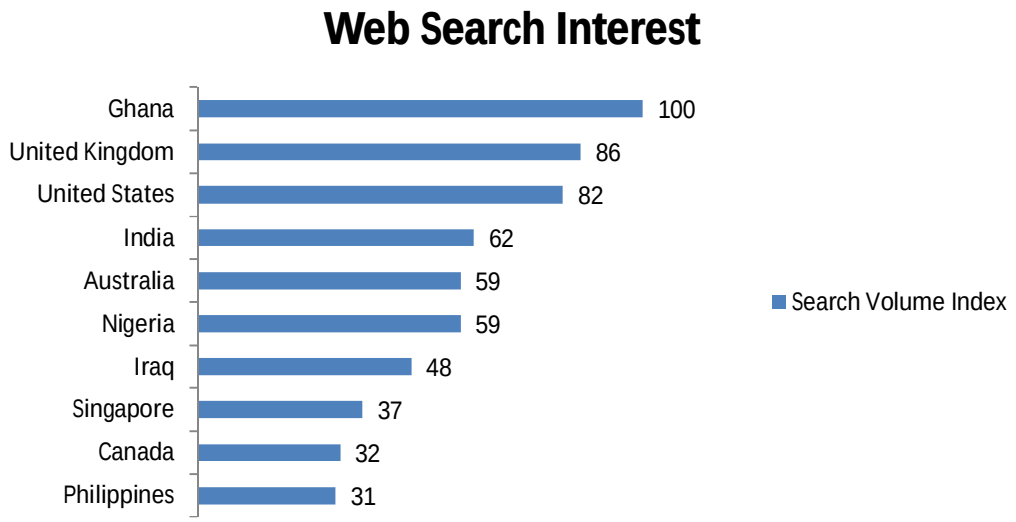
Coomson J. (2006) identifies credit card fraud as the most prevalent cyber crime in Ghana. Using Google's Insights for Search, (which allows users to find out what others are searching for within any location in the world and within any time range, starting in 2004), the researchers performed a query for Google "credit cards" searches worldwide, from 2004 to 2009, the results of which are presented in the graph below.

The data show that the search interest for credit cards in Ghana is higher than in any other country. This interest relates to the level of credit card crime in the country.

Many e-fraudsters in Ghana perpetrate this type of cybercrime. The perpetrators are alleged to be selling stolen credit cards numbers as well as using them to order for products from the United States and Europe. Coomson (2006), reports one of the participants of credit card fraud as saying: "They then go online, place orders and then work in partnership with people in the USA or Europe, whose addresses they ask the illegally purchased goods to be delivered. After delivery, the goods are then sent to them in Ghana"

These scammers buy or steal credit cards and verification numbers from hotel employees and cashiers of super markets, either in the country or from abroad.

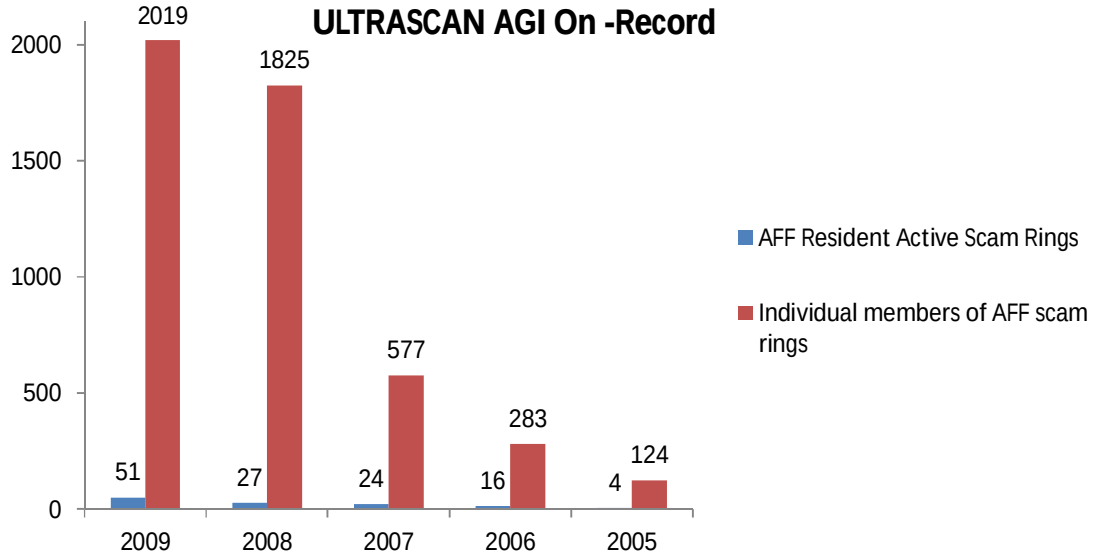
Figure 4: Web Search Interest: Credit Cards



Source: *Ultrascan Advanced Global Investigations, 419 Advanced Fee Fraud Statistics 2009*

Another major form of e-fraud which has taken the country by storm is the Advance Fee Fraud – usually referred to as "Sakawa". The following figure was extracted from the 419 Advanced Fee Fraud Statistics of 2009 by Ultrascan Advanced Global Investigation.

Figure 5: Ultrascan AGI On-Record

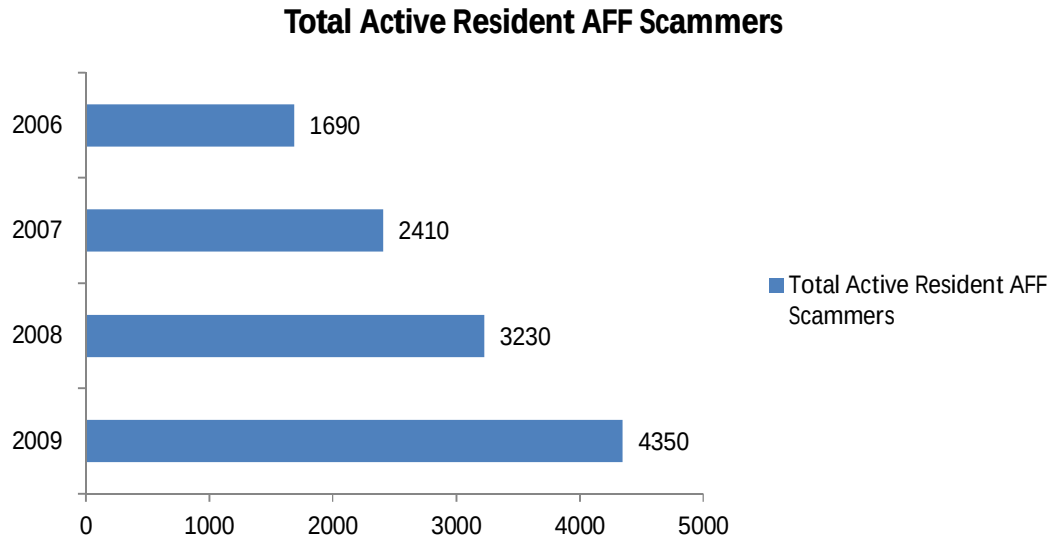


Source: *Ultrascan Advanced Global Investigations, 419 Advanced Fee Fraud Statistics 2009*

Over the 5 year range (2005 to 2009) the number of individual members of advanced fraud scam rings has risen from 124 in 2005 to 2019 in 2009. This just represents the population that commits AFF in rings. (Advanced Fee Fraud Statistics 2009)

The same report gives the total number of active residents engaged in AFF scams. This is represented in figure 6.

Figure 6: Total Active Resident AFF Scammers

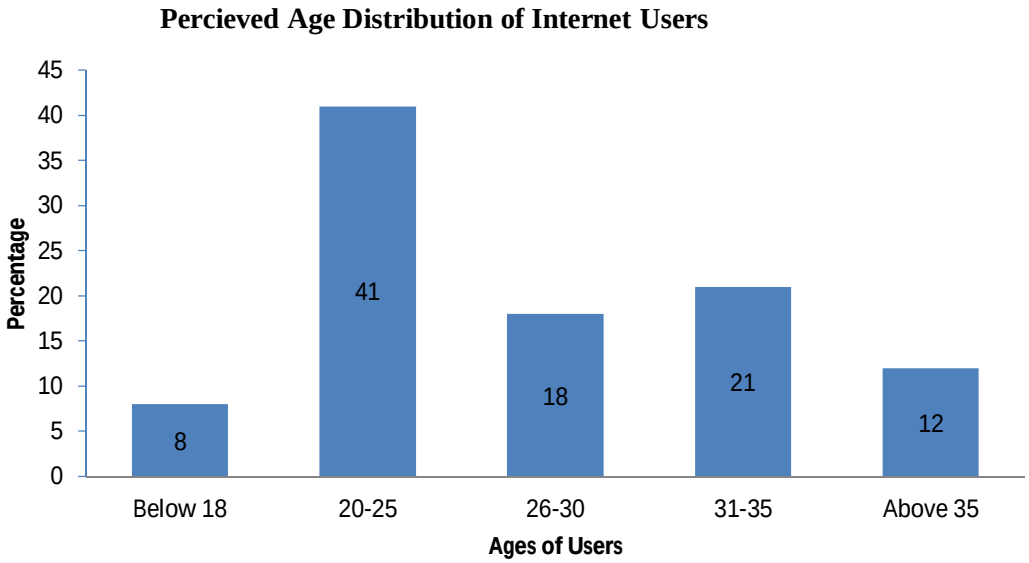


Source: *Ultrascan Advanced Global Investigations, 419 Advanced Fee Fraud Statistics 2009.*

3.2. *Ghanaian Youth in E-Fraud*

In a research by Boateng et al (2010), respondents (Internet Café Operators) were asked to indicate the approximate age of their customers. Figure 7 shows the age distribution of the customers of the cafes according to the Internet Café Operators.

Figure 7: Perceived Age Distribution of Internet Users



Source: AMCIS (American Conference on Information Systems) 2010 Proceedings

The age distribution above tends to suggest that, most of the people who patronize these cafes are young men and were likely to form a majority of perpetrators of internet related crimes.

Boateng et al (2010) observed that more adolescent boys below the age of fifteen are browsing but in answering the questionnaires (presented by the researchers), the café operators tend to have reported a lesser number. In corroborating these findings with the police unit interviewed, they confirmed, that the majority of cyber crime suspects are the youth aged between 20-25 years.

In the same research, the internet café operators could not give the certain sum of those who engage in cyber crime in their cafes, the accent of some of them however suggested they were of Nigerian decent.

3.3. *Tracks of a Cyber Thief*

E-businesses are beginning to recognize the warning signs that indicate possible fraud. Below are some tracks of cyber thieves.

1. Late Night Orders.

A large percentage of fraud orders occur late in the evening or early morning. E-business fraud increases at night. Investigations have shown that 9 out of 10 orders are made between midnight and three in the morning.

2. Orders Placed Outside the Country.

There have been some discrepancies on which countries produce the highest fraud numbers. Russia, West African, and South American countries seem to produce consistent high numbers. The problem with out of country deliveries is that once it is gone, it is gone. A lot of the orders placed by the ‘sakawa’ boys are from overseas.

3. Free/Anonymous E-Mail Services.

It is not every order made with a free/anonymous e-mail service that is fraudulent; approximately 95% of all fraudulent orders investigated were made with these types of services. Fraudsters' using these e-mail services use legitimate ISPs, but they use the free e-mail service for added anonymity. These services will not give information to e- merchants or the police without a subpoena.

4. High Quantity Orders

E-fraudsters will attempt to order large quantities of the same item. A typical order of this nature will be ten 1-carat engagement rings or Six DVDs in one order.

5. High Value Orders

E-fraudsters always order high value items without cognisance to the value of the item ordered.

6. "Ship to" differs from "Bill to"

This is usually a difficult track to follow, especially during festive seasons. Most e-business is built on convenience and the ease of having gifts sent for the customer. Still, this can be a key indicator of a possible fraudulent order. Usually the address that is used to purchase items differs from the bill to the address.

7. E-mail Address

The e-mail addresses that these fraudsters use give some clues. The e-mail addresses, in most cases, will match something in the customer's name. But these fraudsters use extremely crude or cute e-mail names, i.e. Imathief@domainname.com, getbent@domainname.com, etc.

8. Repeated Attempts to Order on The Same Card

There are computer programs that generate credit card numbers for online thieves; however it is not uncommon for a fraudster who has generated a credit card number or stolen one to make numerous attempts on the same credit card keying in different expiration dates or passwords. E-merchants can review repeated and failed order entry attempts.

9. Frequent Calls from Customers

Fraudsters can be really anxious people. They may want to close the deal fast so they can close up shop before they are caught. They may call in repeatedly to check on the status of orders. Some fraudsters call simply to bully and can be extremely obnoxious.

It is important to note that none of these signals are an absolute identifier of fraud. They are indicators of possible fraud.

3.4. *Factors Fuelling E-Fraud in Ghana*

Education in Ghana does not guarantee employment and there is an ever increasing group of unemployed educated young men and women looking for 'white collar work' with unemployment at 20% in 2008 (Online CIA Word Bank Facebook 2010). (Bastian 2001) has written of similar circumstances in Nigeria, with anxieties surrounding jobless, educated young men who are rumored to form cults. As with 'Sakawa', many Nigerians fear the consequences that such behaviour inflicts on their society as a whole as a powerful generation of educated but immoral and violent youth is created (Bastian 2001).

3.5. *Impacts of E-Fraud on the Development of E-Business in Ghana*

Fraud has a huge effect on e-businesses. However, it should be noted that e-businesses are not the only ones affected. Consumers are also negatively affected because of the losses incurred and fraud prevention expenses passed on to the consumer.

E-commerce fraud costs retailers approximately $4 billion each year, according to the most recent results of an annual survey conducted by Cyber source, a provider of electronic payment and risk management services [Goodchild 2009]. The Ghanaian economy, including the growing e-business aspect of it, is increasingly threatened by cyber crime. Multiple studies still show that fraud, security, and privacy continue to be the primary detriment to the growth of e-business. Most economic crimes have a cyber version today. These cyber crimes offer more opportunities to the criminals, with larger payoffs and fewer risks. Websites can be spoofed and hijacked. Payment systems can be compromised and electronic fund transfers to steal funds or launder money occur at lightning speeds. Serious electronic crimes and victimization of the public have caused consumer confidence to waiver in Ghana. These issues have also led to growing privacy concerns and demands. In turn, the reluctance of the Ghanaian public to embrace e-business fully is preventing this new form of business from reaching its potential.

An important impact of these practices is the negative press, loss of credibility and bad image that these practices generate for the nation and for institutions such as the banks and state owned businesses in the country. Currently, it is extremely difficult to transact legitimate business online with a legally acquired credit or debit card. Many companies in the Western world have blacklisted Ghana and many other African countries because they find it cheaper to blacklist all credit card transactions coming from Ghana than to sort out the good transactions from the bad. Such negative blows to our credibility cements the difficulty that we face in our attempts to penetrate the western markets with our products. Even if we succeed in marketing our products, the mediums of transactions will be limited due to mistrust.

Ghana has been short listed among countries with a high rate of cyber fraud, as the country is ranked second in Africa and seventh in the world in cyber-crime or internet crime (myjoyonline.com). Companies have been too careful to engage Ghanaian companies in business deals. This means government is losing revenue especially from the private sector.

E-business has also suffered a major setback due to restriction of Ghana to partake in online trade on most of the international companies' websites.

The government will have to spend scarce resources to combat these crimes. These resources could have been used for other infrastructural development. Human resources is being depleted since most of the youth who indulge in these don't find education and acquiring of skills relevant – they are able to meet their daily lifestyles and live in comfort.

3.6 *Legal Components for Cyber Crime Prosecution*

In Boateng Richard, Longe O., Mbarika V., Avevor I., Isabalija S. R (2010) research, respondents consisted of legal practitioners were asked to indicate the type of law in the criminal code of the Republic of Ghana under which the suspects or internet fraud are charged and whether or not it is appropriate to charge them under these laws. All the respondents indicated there is no law in the statute books that address these types of crime. The police still rely on conventional crime laws on false pretence in the criminal Code Act 29/60 Section 131 and its associate statutes. Crimes committed under these laws are bailable offences and carry lesser punishments which cannot therefore deter the fraudsters from committing cyber offences. The respondents also indicated that it is not wholly appropriate to use this law because the facts of some of the cases do not support the charges made against the suspects under that law hence most lawyers capitalize on such technicalities and have their clients acquitted.

In 2008 the Ghana parliament and the Government of Ghana launched the Electronic Transaction Act (ACT 2008) to regulate electronic communication and transactions. Article 141 of the Electronic Transaction Act (ACT 2008) mandates the security agencies to confiscate accesses of cyber fraudsters.

The Economic and Organized Crime Office was set up by Act 804 of 2010 in line with Article 190 (1((d) of the 1992 constitution to supplement and augment government's effort in the fight against corruption and fraud in the State. The Office was established as a specialized agency of government to monitor, investigate and on the authority of the Attorney-General, prosecute any offence involving serious financial and economic loss to the state and to make provision for connected and incidental purposes.

The mandate of the Office is clearly set out by the EOCO Act. The relevant provisions, at Section 3(1) (a), (b), (c), (d) and (2) S. 12, and S. 13 indicate clearly that the mandate to investigate any suspected fraud is inherent in the Office and can be activated by the Executive Director without reference to any other authority or agency of state.

Ghana has also passed a Mutual legal Assistance Act, 2010 (Act 807) which among others requires persons to submit suspicious transactions reports to the newly established Financial Intelligence Centre.

Government has also set up an emergency Cyber Crime Response Team, to review existing legislature governing the Information Communication and Technology (ICT) activities and strengthen the country's cyber security.

4.0. Conclusion

E-commerce is a phenomenon growing in prominence and it is important to reduce the risks associated with it, especially the problem of 'Sakawa' and electronic fraud. This article made inroads into the impact of e-crime on the development of e-business in Ghana.

With the evaluation of secondary data on 'sakawa' concluded on the following reasons why our youth of today engage in sakawa:

1. Attempts to meet society's expectations.
2. Ambitious lifestyle by today's youth
3. Attempts to get back at foreigners who supposedly bolted away with our raw materials and enslaved our ancestors.
4. Emergence of subculture.
5. Break down of social institutions especially the family.
6. Lack of harsh punishments / legislation for culprits.

Obviously, conscious and serious measures need to be applied to halt and reverse the growing trend of cyber-crime in the country. The culprits are identifiable. They live in communities, and their modus operandi and their lifestyles easily give them away.

Indeed, doing nothing serious to curb this menace may mean that not only will orders from Ghana be blocked by foreign traders, but we could also be shutting ourselves out of future sales to foreign countries. Given the significance of e-business in future international trade and commerce, it would be suicidal for Ghana to establish a bad reputation for itself in that area.

Completely exterminating cyber-crime in Ghana is impossible, just as real crime cannot be completely suppressed. The next best alternative is to prepare for unexpected attacks and damages. Prevention is one way. Precautions, protections and detections should be properly implemented by government, businesses and individuals to remedy the situation of e-crime or e-fraud. Tools and services are available to achieve this.

Given the significant number of e-business counter measures outlined in this article, the opportunity for e-business to grow worldwide on the whole and Ghana in particular is very bright

REFERENCES

1. AMCIS (American conference on information systems) 2010 Proceedings http://vivauniversity.files.wordpress.com/2011/04/cybercrime.pdf 10/07/11
2. Bastian, M.L. (2001) 'Vulture men, campus cultists and teenaged witches: Modern magic's in Nigerian popular media' in Moore, H.L, Sanders, T. Eds. *Magical Interpretations, Material Realities: modernity, witchcraft and the occult in post-colonial Africa*, London & New York: Routledge.
3. Boateng Richard, Longe O., Mbarika V., Avevor I., Isabalija S. R., (2010), "Cyber Crime and Criminality in Ghana:Its Forms and Implications", Americas Conference on Information Systems (AMCIS) 2010 Proceedings, Available online < http://aisel.aisnet.org/amcis2010/507>
4. Coomson, J. (2006) Cyber crimes in Ghana, *Ghanaian Chronicle*, 4 October 2006. [Online]. Available: http://allafrica.com/stories/200610040856.html
5. ECIS (European Conference on Information Systems) 2004 Proceedings http://is2.lse.ac.uk/asp/aspecis/20040168.pdf viewed 09/07/11
6. E-Commerce security: Attacks and preventive strategies http://www.ibm.com/developerworks/websphere/library/techarticles/0504_mckegney/0504_mckegney.html viewed 10/07/2011
7. Effects of Cyber Crime | eHow.com http://www.ehow.com/about_5052659_effects-cyber-crime.html#ixzz1teE2ycrd
8. Goodchild, J. (2009). "E-Commerce Fraud: the Latest Criminal Schemes," *NetworkWorld*. 16 July <http://www.networkworld.com/news/2009/071609-e-commerce-fraud-the-latest-criminal.html>
9. Graham, T (2002), 'Dispute resolution: E-Fraud and Jurisdiction' http://www.tjguk.com/topical/litigation/efraud_and_jurisdiction_winter2001.html
10. http://www.ghanaweb.com/GhanaHomePge/NewsArchive/artikel.php?ID=159265, viewed on 12/07/2011)
11. http://www.google.com/insights/search/?hl=en-GB#q=credit%20cards&cmpt=q viewed on on 12/07/2011
12. http://www.myjoyonline.com/pages/news published july2013 19:50 GMT
13. http://www.telegraph.co.uk/news/worldnews/africaandindianocean/ghana/7664254/Police-arrest-suspected-romance-fraudster-who-posed-as-US-soldier.html, viewed on 12/07/2011
14. Longe, O., Ngwa, O., Wada, F., Mbarika, V. and Kvasny, L. (2009) Criminal Use of Information and Communication Technologies in Sub-Saharan Africa: Trends, Concerns and Perspectives, *Journal of Information Technology Impact*, 9,3, 155-165
15. Oumarou, M (2007) Brainstorming advanced fee fraud: 'Faymania' – the Camerounian experience, in N. Ribadu, I. Lamorde and D. Tukura (Eds), *Current trends in advance fee fraud in West Africa*, EFCC, Nigeria 33–34.
16. Pati, P. (2003) Cybercrime, New Delhi [Online]. Available: http://www.naavi.org/pati/pati_cybercrimes_dec03.htm
17. Thomas, D.R. (2003). A general inductive approach for qualitative data analysis, University of Auckland