The Impact of Cybercrime Related Offences on E-Commerce Transactions in Cameroon

Anoumbuandem Benvolio Lekunze

Faculty of Laws and Political Science, University of Buea

DOI: https://doi.org/10.51584/IJRIAS.2025.100500049

Received: 28 April 2025; Accepted: 08 May 2025; Published: 09 June 2025

ABSTRACT

Electronic commerce (e-commerce) transactions have gained global significance and widely used nowadays to conduct businesses in cyberspace. The introduction of e-commerce in Cameroon and electronic payment methods have several advantages in completing commercial transactions. Despite the advantages, cybercrimes pose high risks and threats to its existence. Cybercrimes in e-commerce related transactions have caused socio-legal and economic problems in Cameroon. The article adopts the qualitative research methodology with the use of the doctrinal method where a survey was carried out. It is based on the utilitarian, transaction cost and the rational choice theories. The research is conducted at a time that cybercrimes are on a rise and adversely affecting e-commerce transactions in Cameroon. The major finding shows that cybercrimes have caused loss of trust and confidence in e-commerce transactions within Cameroon and abroad. The findings also reveal that there is a declining rate at which people are willing to carry out e-commerce transactions in Cameroon because of cybercrimes. It has also been found out that more than 60% of persons between the ages of 16 and 35 in some major Cameroonian cities are either involved in e-commerce related cybercrimes or have been involved in the past. The conclusion drawn is that cybercrimes have adversely affected e-commerce transactions in Cameroon. The article recommends some measures like the institution of a proper home address system, the assignment of social security numbers to Cameroonians and strict procedural rules should be enacted to improve the situation. The research is beneficial to the education community, the judiciary, the government, and foreigners willing to carry out their businesses in Cameroon through e-commerce.

Key words: Impact, Cybercrime, E-commerce, Transactions

INTRODUCTION

Crimes are frequent occurrences in every human society and operate as a core concept in modern society.[1] The introduction of the internet to the public on the first of January 1983[2] has facilitated the commission of some crimes through online communication portals that were not initially foreseen by the legislator. The first recorded history of cybercrime was in 1834 when the French telegraph system was hacked, and access gained to financial markets through stolen data.[3] The act of committing cybercrime involves different elements, tools and processes as opposed to conventional crimes that may not raise issues of jurisdiction and proof. This is because cyberspace is vast and unlimited to a particular geographical region or country.

Cybercrime can be defined as a wide range of criminal activities that are carried out using digital devices and networks.[4] It is also a collection of offences against computers and computer systems.[5] A computer can be the object of commission or a target. Cybercrime can also be any criminal activity that uses a computer either as an

[1] Chris H., et al, Criminology: Oxford, Oxford University Press, (2005) p.1.
[2] www.usg.edu (accessed on the 18/04/2025). January 1, 1983 is considered the official birthday of the Internet. Prior to this, the various computer networks did not have a standard way to communicate with each other. A new communications protocol was established called Transfer Control Protocol/Internetwork Protocol (TCP/IP). This allowed different kinds of computers on different networks to "talk" to each other. ARPANET and the Defense Data Network officially changed to the TCP/IP standard on January 1, 1983, hence the birth of the Internet.
[3] www.bluevoyant.com (accessed on the 17/04/2025)
[4] Cybercrimes it should be noted are common in the domain of commercial transactions than others.
[5] Payne, Brian K., The Handbook of International Cybercrime and Cyber evidence: London, Palgrave Macmillian, (2020) P.3.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue V May 2025

instrumentality, or a means for perpetuating further crimes. It can take the form of cyber theft or other related illegal activities targeted on humans and property.[6] This article focuses on the impact of cybercrimes in electronic commerce (e-commerce) transactions in Cameroon because available literature on the impact of cybercrimes on e-commerce in Cameroon is limited. Examples of cybercrimes include but not limited to; hacking, cyber stalking, defamation, email bombing, data diddling, salami attacks, denial of service attack, virus and worm attacks, internet time thefts etc. It may be observed that e-commerce transactions as the name signifies operate in cyberspace through electronic data interchange (EDI)[7] and is not always void of crimes.

E-commerce can be through engaging in online shopping, mobile apps conversational commerce via live chat, chatbots, and voice assistants.[8] It can be through Business to Business (B2B), Business to Customer (B2C), Customer to Customer (C2C) and Customer to Business (C2B). Electronic commerce was first used as a phrase by Robert Jacobson in 1984 in the California Electronic Commerce Act.[9] He referred to it as the process of conducting sales transactions over the internet with the use of electronic communications and digital information processing technologies, to create, transform, and redefine relationships for value between people and organizations. It is also defined as the practice of buying and selling goods and services through online consumer services on the internet.[10] It is one of the ways that companies and individuals carry out their business to maximize profits while reducing fixed cost over a broad range of assets. It also minimizes transport costs from central business districts.[11] It was reported in January 2025 that there are about one thousand two hundred and three e-commerce websites in Cameroon. Some examples include; glotelho.cm, camoo.hodsting, iziway.cm, limarket.net, Cameroon-tribune.cm etc.[12]

There are several advantages associated to e-commerce transactions. Some of these advantages are; fast buying processes, low advertising costs, product price comparison, different payment options etc. Despite these advantages, cybercrimes in e-commerce have led to loss of profits, trust and confidence amongst business counterparts. There are efforts in Cameroon to combat cybercrimes through legislation and technology, but this has not so far led to any significant impact. This can be attributed to low internet speed, weak digital rights management systems[13] and circumventing technologies.

Cybercrimes and related offences in commercial transactions have in the past years experienced a rise in Cameroon due to an increase in the proliferation of the internet. The cost of procuring electronic devices is low. Lockdowns during the outbreak of the COVID-19 pandemic also contributed to this phenomenon. Cybercrimes became popular in Cameroon around 2005 before the enactment of the 2010 laws on cyber criminality and electronic commerce. This can be demonstrated by the earlier cases of; *The People v. Obi Roland,*[14] *The People v. Nfang Macknight,*[15] *The People v. Mbah Valery,*[16] *The people of Cameroon v. Tamukum Fonjiyang Ferdinand & one other,*[17] *The people* of *Cameroon & another v. Tita Njina Kevin Ndango.*[18] All these cases preceded the 2010 Laws on cyber criminality and electronic commerce in Cameroon although some of these cases were reported later. It can be observed in these cases that the civil parties were never present in court. That is notably one of the reasons that has led to a sharp rise of cybercrimes in Cameroon.

[6] Brayan A. Garner, Black's Law Dictionary: Minnesota, West Group, (1999) P. 392.
[7] Ibid p. 531.
[8] www.venturebeat.com/ai/how-to-prepare-your-products-and-brand-for-conversational-commerce/ (accessed on the 16/04/2025).
[9] See the California Civil Code Section 1789 et. Seq. which is also the electronic commerce Act of 1984.
[10] Op. cit. note 4 p.530.
[11] This can be explained by the Von Thunen Theory of agriculture that was developed by Johann Heinrich in 1826. This model predicts human behaviour in terms of landscape and economy based on meticulous mathematical calculations and observations. It explains transport cost from the geographical location of farms to a central business district (CBD). Although it is a theory in agriculture, it relates to e-ecommerce today because the principal objective of e-commerce is to minimize transaction costs from where goods and service originate to where a consumer is located.
[12] www.brandnav.io/reports/counties/cameroon (accessed on the 24/04/2025)
[13] It refers to technical ways of securing data with the use of passwords, cryptography and steganography.
[14] CFIB/55C/2008(Unreported).
[15] CFIB/76C/2009(Unreported).
[16] CFIB/255/2010(Unreported).
[17] (2014) 2 SLR.
[18] (2010) CCLR 1-126

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue V May 2025

The first legislations on cybercrimes and e-commerce in Cameroon were enacted in December 2010 because of frequent occurrences of cybercrimes. Most of the crimes were related to false commercial transactions[19] disguised as legitimate business transactions.[20] This is why the cyber criminality law and the electronic commerce laws in Cameroon were enacted in the same year. This research therefore simultaneously dwells on the impacts of cybercrimes on e-commerce transactions for the above reason.

The cyber criminality law in Cameroon provides the legal framework for investigating and prosecuting cybercrimes alongside the Cameroonian Penal Code and the Criminal Procedure Code (CPC). It elucidates the types of cybercrimes which are; unlawful interception of communications, hacking, computer related fraud, offences relating to child pornography etc. The law is adjectival and procedural because it provides rules for investigating and prosecuting cybercrimes with international co-operation.

The 2010 law on electronic commerce in Cameroon on the other hand lays the legal foundation to e-commerce in Cameroon.[21] This law was precipitated because of the rapid emergence of e-commerce platforms that followed global trends.

Cybercrimes in Cameroon exist not only in e-commerce transactions but also in other criminal acts like defamation, false pretense, theft, cyberstalking and hacking. Law N° 2010/012 of 21st December 2010 relating to cybersecurity and cyber criminality in Cameroon criminalizes cybercrimes jointly with law N° 2016/007 of 12 July 2016 relating to the Penal Code.[22] While Law N° 2010/021 of 21 December 2010 on electronic commerce in Cameroon establishes offences and punishments for violating the provisions of e-commerce rules. The impact of cyber criminality on e-commerce in Cameroon is huge coupled with the fact that a majority of the country's citizenry is not computer savvy. This has led to some legal problems at the micro and macro-economic levels like; increased bribery and corruption and a general increase in crime wave.

Statement of the problem

The are many problems associated to cybercrimes and e-commerce in Cameroon. There is the absence of official home addresses and no social security numbers in Cameroon. The lack of digital home addresses and social security numbers often frustrate the work of investigating officers.[23] There is also loss of trust and confidence in electronic based commercial transactions in Cameroon because many payments are unsecured.[24] The level of criminal activities across the country has also increased because illicit profits derived from cybercrimes are sometimes used in furtherance of other crimes like drugs abuse, bribery, corruption, crimes of moral integrity, public drunkenness etc.

Cybercrimes in related e-commerce transactions have also led to a high level of arbitrary arrests and torture without tangible evidence. Bribery and corruption is also another problem commonly found in e-commerce related cybercrime cases. There is also low-level attention on international co-operation to combat e-commerce related cybercrimes in Cameroon. These aspects have led to an atmosphere of shame and fear in Cameroon. The failure to properly define the powers of the National Financial investigation agency (NFIA)[25] and the National Agency for information and communication technologies (NAICT)[26] in Cameroon is also problematic.

Theoretical and Conceptual frameworks

[19] Section 318 of Law N°2016/007 of 12 August 2016 on the penal code.

[20] Cybercrimes in Cameroon were officially recognized as a legal issue with the enactment of law N°2010/012 of December 2010 which defines cybercrime offences and provided penalties. Before this law, many instances of cybercriminality were addressed under the penal code.

[21] Law N° 2010/021 of 21 December 2010.

[22] Section 219 of the Penal Code.

[23] This makes aspects like investigations, the execution of summonses and arrests strenuous because deliveries are usually at the post offices or in other locations on call.

[24] Return policies are highly ineffective in Cameroon and are hardly embodied in commercial contracts. So the aspect of fear creeps into customers' minds.

[25] Popularly Known in Cameroon by its French acronym as ANIF

[26] Popularly Known in Cameroon by its French acronym as ANTIC

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue V May 2025

This article is based on several theories that explain the reasons why cybercrimes are committed and targeted most especially towards e-commerce. Some of the selected theories are the theory of utilitarianism, the transaction cost theory and the rational cost theory.

The utilitarianism theory

This theory was propounded by John Staurt Mill in 1816. He believed that happiness was the only thing humans do and should desire for their own sake. He believed that because happiness is the only intrinsic good, and since more happiness is preferable to less, the goal of ethical life is to maximize happiness. Jeremy Bentham and John Staurt Mill called it ''the principle of utility'' or ''the greatest-happiness principle.'' In the context of this article, cybercrimes in e-commerce satisfy the cravings, wellbeing and the happiness of the perpetrators. Therefore, the drive to satisfy personal ego and happiness by offenders may drive them to desire the benefits of defrauding others by way of committing cybercrimes in e-commerce transactions. This theory aligns with the Resourceful Evaluative Maximizing Model theory that views individuals as rational actors who are always seeking to maximize their own utility or wellbeing within a given set of constraints. It shows that individuals always strive to find the best possible outcome due to constraints in their resources.[27]

Transaction cost theory

This theory was introduced by John R. Commons in 1931.[28] It is cost incurred when carrying out trade. The costs are associated to those in running the economic system of a company and the total costs of carrying out transactions. It also includes the cost of planning, deciding, changing plans, resolving disputes, and after-sales costs. According to the author, the determinants of transaction costs are frequency, specificity, uncertainty, limited rationality, and opportunistic behaviour. One of the objectives of e-commerce is to significantly reduce transaction costs by way of electronic data interchange (EDI).

The Transaction Cost Theory (TCT) focuses on minimal effort on resources and the cost required for parties to exchange their goods and services. The objective of this theory is to maximize transaction performance while minimizing costs.[29] This is the main objective of e-commerce. This theory can be compared to the Von Thunen model developed in 1826[30] that dwells on transaction cost of farm produce to the central business district (CBD). The sales price of the produce is determined by the distance of the central business district and where production takes place. This theory is related to e-commerce because of the distances that goods and services are located and the distance that they have to be moved for supplies. E-commerce in consideration to this model leads to reduced cost, irrespective of where the goods are manufacture and where they are delivered. This is opposed to transactions that are concluded in a manner that parties have to travel over long distances to carry out negotiations or shopping in real world.

Rational choice theory.

This theory was propounded by Adam Smith in 1776[31] and later articulated by the sociologist George Homans in 1961.[32] The theory is based on behavioral psychology.[33] The theory involves achieving a goal using the most cost-effective method without reflecting on the worthiness of that goal. The goals may be self-regarding, or selfish.[34] The theory provides guidelines that help to understand economic and social behaviour. It is also used in criminology. It helps to predict the outcome and pattern of choice and assumes that individuals are self-interested when decisions are based on optimizing preferences by balancing costs and benefits. This phenomenon is common in e-commerce where many options are available in online shopping that leads to different choices and preferences. The objective of cybercriminals in e-commerce are usually self-centered without regards to the

[27] Wartiovaara, M. Rationality, ''REMM, and Individual Value Creation.'' Journal of business Ethics, Vol 98, (2011), P641-648.
[28] Williamson, O. E., Outsourcing, ''Transaction Cost Economics and Supply Chain Management, Journal of Supply Chain Management'' Vol 44, (2008), P. 2-82,
[29] www.sciencedirect.com(accessed on the 23/04/2025)
[30] Johann Heinrich von Thunen (24 June 1783 – 22 September 1850), was a prominent nineteenth-century economist in Germany
[31] Adam Smith was a Scottish philosopher and economist born in 1723 who wrote on the wealth of nations.
[32] George Homans was an American Sociologist born in 1910 and wrote on social behaviour and exchange theory.
[33] www.britannica.com/money/rational-choice-theory(accessed on the 23/04/2025)
[34] Ducan S., Rational Choice and Interntional Relations: London, Sagge (2013) p.87.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue V May 2025

consequences caused to their victims after depriving them of their wealth. The theory is also related to crime because an individual can decide to commit an offence and be caught or takes the risk to commit an offence and go free. This is a typical phenomenon in e-commerce related cybercrimes where it is difficulty to catch perpetrators in the act.

RELATED LITERATURE

Some authors have written independently in the areas of cybercrime and e-commerce. They have established some connections between cybercrimes and e-commerce. While few authors have highlighted the impact of cybercrimes on e-commerce transactions. They have not critically examined the metaphoric relation between the two. The same sanctions that exists in conventional crimes in commercial transactions exist under cybercrimes in e-commerce transactions. What happens offline is the same as what happens online with the difference being the mode and interface used in carrying out the same act.

Lawrence Lessig (1999), a Harvard Law professor has written extensively on the need to create a uniform code to regulate cyberspace. He emphasized that every age has its potential regulator which is related of the threat of liberty. He elaborates that; laws are obeyed out of fear and injustices of the market. The author emphasized on the enactment of a uniform code in cyberspace to regulate software and hardware. He explains that the code, or architecture, sets the terms on which life in cyberspace is experienced. It determines how easy it is to protect privacy, or how easy it is to censor speech. It determines whether access to information is general or whether information is zoned to affect who sees what or what is monitored. He insisted that a basic code of the Internet should implement a set of protocols. The code as assumed by the author should inform on the behavior that individuals ought to portray on the internet. His work does not specifically caution e-commerce transactions as an aspect that works through cyberspace and susceptible to cybercrimes. The author further demonstrated that for this code to be effective, governments should be in the same level of development since online dealings have no political boundaries.

Billy Henson (2011), dwells on the fears caused by cybercrimes because of victimization. The author examines the relationship between risk in cyberspace for fear of being a victim of cybercrime. His analysis is based on information collected from undergraduate students at the University of Cincinnati. The major finding in his research reveals that many people fear to become victims of cybercrimes. He further emphasizes on the category of offenders and their behavioral pattens in relation to status and gender. His work examines behavioural frequencies that have great effects on the levels of fear because of cybercrime victimization. He agrees that fear and victimization in cyberspace are based on perceived risks. His work doesn't analyze how these fears can be allayed to encourage e-commerce. This research agrees with the view of this author because e-commerce transactions have been declining due to the high frequency of related cybercrimes.

Rainer Bohme and Tyler Moore (2012), dwell on cybercrimes in online shopping and how to prevent them. Their main finding was that cybercrimes have caused a decline in transactions like; online banking, online shopping. They concluded that people who do not know about cybercrimes are more likely to engage in e-commerce transactions like online shopping. Their work is mostly limited to online shopping meanwhile e-commerce is broader.

Szde Yu (2014), analyzes victimization experience, perceived risk of victimization and perceived risks caused by cybercrimes on e-commerce. The research analyzes the aspect of fear and cybercrime. The research also examines four kinds of cybercrimes and dwell on the relationship between cybercrime and fear.

Wekundah Ruth Nangechey (2015) focused on the different cyber attacks on small and medium enterprises. The research is unique because it uses the quantitative and qualitative research methodologies. It was found out that most small and medium enterprises do not allocate enough resources to combat cybercrime attacks. The research falls short to adequately examine the various ways that cybercrimes could be managed to improve e-commerce transactions.

Yushawu Abubakari (2020) demonstrates the way people lose many opportunities for fear of being scammed. The author reveals the reasons, impacts and limitations of cybercrime policies in Anglophone West Africa. He

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue V May 2025

also demonstrates the ways that cybercrime perpetrators lose focus in education. He attributes this to the growth of cybercrimes that are associated to economic strains[35] and corruption at the governmental level. The author considers hindrances in cybercrime policy because of corruption, government interference, ineffective implementation of cybercrime laws and inconsistencies in the content of cybercrime policies. His research focused on Ghana, Nigeria, and Sub-Saharan Africa as a representative sample for Anglophone West Africa. According to the author, this is because the prevalence of internet fraud in West Africa is centred around the Anglophone West African counties like; Ghana, Nigeria, Liberia, Sierra Leone, Gambia and part of Cameroon, with Nigeria and Ghana being the most notorious.

André Boraine and Ngaundje Leno Doris (2019) wrote on the fight against cybercrime in Cameroon. They focused mainly on the conflict in the Anglophone regions of Cameroon and showed a link between the conflict and the increased rate of cybercrimes due to the conflict. They examined the role of the government of Cameroon in the fight against cybercrimes and analyzed some of the legal provisions used to combat cybercrimes in Cameroon. Their paper examined why cybercrimes are prevalent in Cameroon and recommends measures that can be put in place to combat cybercrimes in Cameroon. They did not show the direct impact of cybercrimes on e-commerce transactions in Cameroon. Their paper raises awareness and contributes to knowledge in data protection rules, especially among investigating officers, students, specialists, and non-specialist legal practitioners.

Most available literature as examined above is either focused on cybercrime or e-commerce. This article shows the direct impacts of cybercrimes on e-commerce transactions in Cameroon and makes recommendations.

Common types of e-commerce related cybercrimes in Cameroon.

Cybercrimes in e-commerce transactions in Cameroon caused an approximate loss of 12.2. billion francs CFA in 2021 with scamming and phishing accounting for approximately half the amount.[36] There are different types of e-commerce related cybercrimes that affect Cameroon and the world. It may be observed that the nature of cyberspace communications does not limit cybercrimes to particular geographical territories. A person may be in a country and commit cybercrimes across different countries with different systems of law. Therefore, there is need for international co-operation to combat cybercrimes especially e-commerce related cybercrimes. This same reason accounts for the absence of complainants in legal proceedings and the growth of cybercrimes.[37] Most cases of cybercrimes in Cameroon are oriented towards financial gains that occur in e-commerce transactions.

Scamming.

Scamming originates from the word scam. It is a dishonest plan to make money or taking advantage by tricking people. It becomes a scheme if the plan is in a large scale. Scheming is relatively rare in Cameroon.[38] Scamming is also a confidence trick to defraud a person or group after gaining their trust by taking advantage of a combination of factors like the victim's naivety, compassion, vanity, confidence and greed.[39] According to a 2021 report of the Cameroonian Ministry of Post and Telecommunications (MINPOST), the rate of scamming was 60% in Yaounde, Douala, Buea and Noun amongst unemployed young people aged between 16 and 35 years.[40]

Scamming is not a new phenomenon but has grown with the proliferation of ICT tools and the internet. In ancient Greece, cups and balls trick were used as forms of deception and in same Greece, a ''confidence man'' called

[35] See the strain Theory
[36] Op.cit. note 30
[37] One of the reasons behind lack of will in Cameroon to prosecute cybercrimes is because the victims are sometimes citizens of foreign countries and lack interest to prosecute in Cameroon due to some legal challenges, cost and fear. This aspect permit bribery and corruption since the victims are not usually available in Cameroon.
[38] Op.cit. note 6 p. 1346.
[39] Haung L., Orbach B., ''Con men and their enablers: The anatomy of confidence games'' Social Science international Quarterly (2018) vol 4. P.85.
[40] www.minpostel.gov.cm (accessed on the 21/04/2025).

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue V May 2025

Thompson who was a swindler asked his victims to express confidence in him by giving him money rather than gaining their confidence in a more nuanced way. He was not successful and was arrested in July 1849.[41]

E-commerce related cybercrimes became noticeable in Cameroon in 2005 before the enactment of the 2010 law on cyber criminality. Before then, courts relied mostly on the Penal Code[42] to adjudicate such cases as was seen in the case of *The People v. Obi Roland.*[43] This was a case of scamming that was heard by the Court of First Instance Buea in 2008. Section 318 of the Cameroonian Penal Code was used as basis of the judgement. The accused was found guilty and sentenced to six years imprisonment. This was the same position held by the court in *The People v. Nfang Macknight,*[44] where the accused was found guilty for similar reasons.

Even though the court had found the accused persons guilty in the abovementioned cases, surprisingly, many of such cases hardly filed in the Cameroonian courts in our present day. The procedure in determining cybercrime cases is often riddled with incompatibilities like the violation of rights under sections 3 and 8 of the CPC that have led to the discharge of some accused persons as was in the cases of *The People v. Mbah Valery,*[45] *The people of Cameroon v. Tamukum Fonjiyang Ferdinand & one other.*[46] It can be observed that because of the high level of bribery and corruption in e-commerce related cybercrime cases in Cameroon, courts are hardly seized. This is because most scammers and investigating officers prefer to engage in corrupt practices. However, when a complaint decides to prosecute his case by filing a civil claim, such scammers and officers are usually overwhelmed. This was so in the case of *The people* of *Cameroon & another v. Tita Njina Kevin Ndango.*[47] where the Court of First Instance Buea found the accused guilty of all the counts in the charge because the complainant travelled from Switzerland to attend the hearing.

Phishing

It refers to a type of scam where victims are tricked to reveal sensitive information. It may also be by installing a malware that contains salami attacks, viruses and worms. These malwares can mirror a targeted website.[48] It may be done with slight alteration in the spelling and numbers of a website to slightly resemble the original website. Some e-commerce user may not easily identify this trick. There are several types of phishing ways that include e-mail phishing, [49] that are often delivered through e-mail spams and spear phishing that uses personalized messaging. Others include voice phishing,[50] Short message service (SMS) phishing, man-in-the-middle (MitM) phishing and quick response code (QR) [51]phishing.

Phishing is commonly used in Cameroon on mobile networks where victims are called or sent a bait text message. The fake messages are usually on grounds of erroneous financial deposits into the victims' mobile money accounts. The perpetrator meanwhile has logged the telephone number of the victim into the mobile operator's version of desktop application (APP). The perpetrator then tricks the victim to verify his mobile account details by entering his passcode for a refund with a promise of reward. If the victim makes a request for a mobile money service on his account and enters his passcode, same is simultaneously communicated to the perpetrator's desktop app where he gains access to withdraw or transfer funds.

This aspect is notorious in Cameroon and almost all mobile telephone users in Cameroon have experienced this phenomenon with some people falling for the trick. This aspect generates fear and also distorts the smooth functioning of e-commerce carried out by mobile telephone companies in Cameroon. Recoveries have been done

[41] Op.cit note 29.
[42] Law N°2016/007 of 12 July 2016 on the penal code of Cameroon.
[43] CFIB/55C/2008(Unreported).
[44] CFIB/76C/2009(Unreported).
[45] CFIB/255/2010(Unreported).
[46] (2014) 2 SLR.
[47] (2010) CCLR 1-126
[48] Jansson, K., von Solms, R. "Phishing for phishing awareness."Behaviour & Information Technology. Vol 32 No 6 (2011).
[49] www.theatlantic.com(accessed on 23/04/2025)
[50] Griffin, Salade E., Rackley, Casey C. ''Vishing''. Proceedings of the 5th annual conference of information security curriculum development. (2008) p.33.
[51] QR code means quick-response code that is a two-dimensional matrix barcode invented in 1994 by Masahiro Hara in the Japanese Denso Wave company for labelling automobile parts.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue V May 2025

at some instances where the offenders have been successful tracked. This has been possible because it is compulsory for customers to register their telephone numbers in Cameroon.

Bank Card Skimming

This happens when technological devices are installed on or inside automatic teller machines or other sales points. Cybercriminals can capture card details and replicate them by using this technic.[52] It is also a tactic that criminals use to obtain sensitive information from a debit or credit card for subsequent use.[53] Bank card skimming is not very common in Cameroon because of the scarcity of the technological devices used and because most ATMs and sales points are secured with cameras and guards.

Socio-legal impacts of cybercrimes on e-commerce transactions in Cameroon.

Cybercrimes have many negative consequences on businesses and e-commerce users ranging from loss of confidence to bankruptcy of businesses and other social ills across Cameroon. Fright is an element that affects the physical and psychological dispositions of every human being. It erodes confidence and pushes people to do cost benefit analysis thereby leading some people to prefer ‘‘on the spot’’ cash payments.[54]

The proliferation of cybercrimes in e-commerce transactions can be explained under the utilitarian and the rational choice theories.[55] Human nature tends to situate people in a position that maximizes their satisfaction even if it means to engage in irrational choices that at times may achieve a positive goal without fear of the consequences. The utilitarian view considers satisfaction as a factor that can overshadow rational behavior. This explains why a majority of youths and young people in Cameroon in some places like Buea and Bamenda have adopted scamming as a trade. E-commerce related cybercrimes have also grown rapidly in these areas because of the socio-political conflict in the English-speaking regions of Cameroon.

This situation is further aggravated by a high unemployment rate amongst the youths, a low minimum wage level across the country[56] and a general low salary scale in Cameroon. Most of the youths in these areas of Cameroon especially the females open fake online shops purporting to do e-commerce transactions through social media platforms to mask the illicit sources of their income. E-commerce related cybercrimes were mostly committed in the past by males who engage in deceptive tricks by electronically producing rare images of objects and animals that never existed in nature.

Easy internet access at affordable costs in Cameroon has surged the rate of scamming and phishing. A survey of 250 respondents carried out by the author between January to April 2025 at the Molyko neighborhood in Buea revealed that at least 60% of the youths in Molyko are involved in e-commerce related cybercrimes. The data collected also revealed that 10% of the perpetrators were females while 50% were males ranging from the ages of 16 to 35. It was also observed that most of the victims are people residing in Molyko who are known by the cybercriminals. A few victims were unknown by the perpetrators while some of the victims resided in different cities of Cameroon and abroad. The survey also found out that the illicit financial benefits derived by the cybercriminals significantly varied and that the activities of the perpetrators involved mostly scamming and phishing.

The tables below illustrate the percentage of youths in Molyko involved in e-commerce related cybercrimes. Table one shows the total percentage while table two shows the percentage of males and females involved within the total percentage of youths involved.

[52] www.fbi.gov>common -frauds-and-scams>skim (accessed on the 22/04/2025)
[53] www.brightbridge.com(accessed on 22/04/2025)
[54] Many purchasers in Cameroon prefer to buy and do spot payments in cash for products that they can see and fill. This is the reason why most people in Cameroon move with cash despite the attendant risks.
[55] See the Rational theory supra.
[56] The minimum wage in Cameroon is 46,939frsCFA less than what obtains in other neigbhouring African countries.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue V May 2025

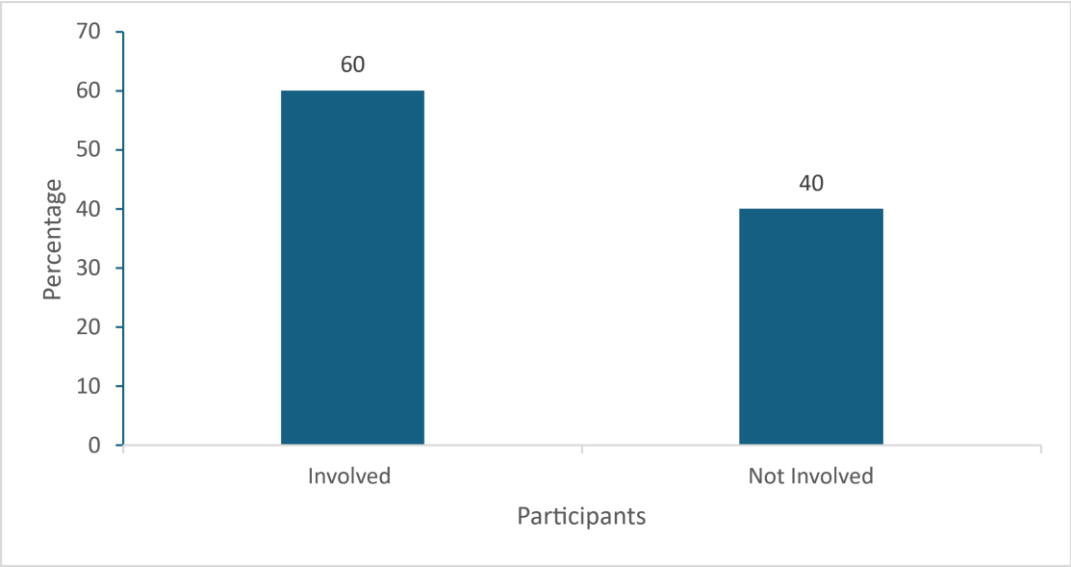

Figure1.

Percentage of youths in Molyko involved in e-commerce related cybercrimes.

Sample Size: 250

Age Range: 16-35

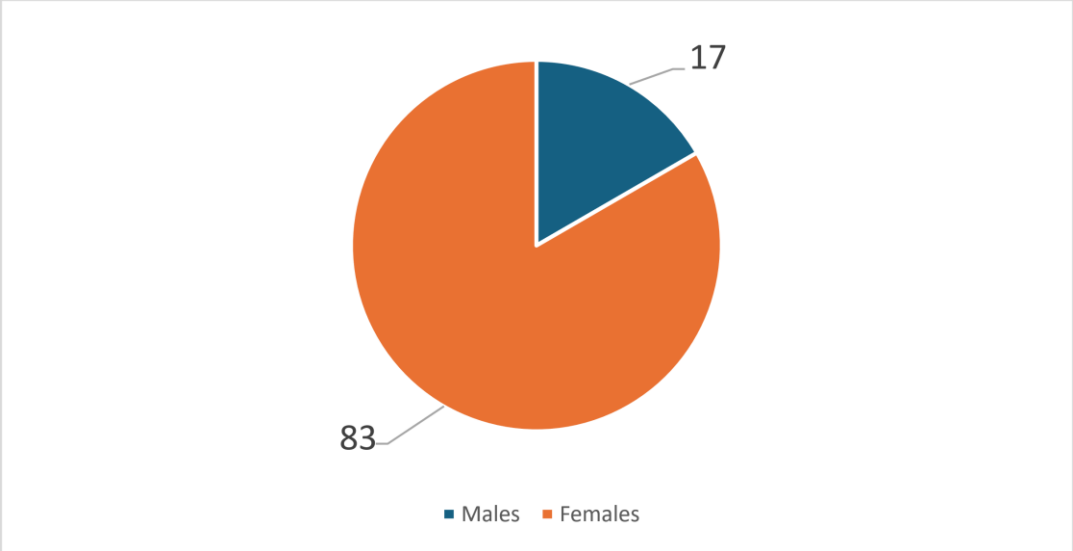

Figure 2.

Gender of Youths in Molyko involved in e-commerce related cybercrimes.

Male /Females.

The survey concluded that most of the youths in Molyko got involved mainly because of ego. Other reasons being peer pressure, strain and the insignificant number of prosecutions because of corrupt practices. It was also concluded that most of these cybercriminals are still actively involved in scamming and phishing and still perfecting their skills. It was also discovered that many youths have dropped out of school as observed by

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue V May 2025

Yushawu Abubakari in his article in 2020.[57] While some youths who have been submerged by cybercrimes paid others out of their illicit gains to impersonate them during examinations.[58]

Occultic practices[59] are also common with dire consequences amongst cybercriminals in Cameroon because most youths with low intellectual capacity are fooled to believe that their successes are dependent on such practices. Occultic practices as such has led to some fatalities and the emergence of organized gangs that at times jointly contribute bribes to ‘‘make a way out’’ for their counterparts in trouble. The level of these occultic practices extend to other social aspects like homosexuality, Lesbianism, incest and sexual activities under the same roof.[60]

All these factors have increased the level of illiteracy amongst the youths in Cameroon. Meanwhile the Cameroonian government has been sacrificing to educate its youths by subsidizing primary, secondary and university education throughout the country.

The Proliferation of other offences due to e-commerce related cybercrimes.

Illicit wealth derived from e-commerce related cybercrimes in Cameroon has led to the proliferation of other offences like drugs abuse, prostitution, public drunkenness, sexual offences, defamation, violence, corruption, identity theft, assault, battery reckless driving etc. Unexpected wealth can lead to psychopathic tendencies especially amongst youths whose metal capacities are still developing. This aspect was also observed in the survey conducted.

Loss of trust and confidence by e-commerce users

It is common today to see most youths in Cameroon who are living a flamboyant lifestyle while riding cars of a particular mark without any proof of financial means. This attitude is directly linked to the high rate of e-commerce related cybercrimes and corrupt practices. Cameroon’s corruption index according to transparency international in 2024 was 26 points /100. It was far higher than most countries in the world.[61] These results can be partially attributed to cybercrimes in e-commerce and the accompanying frivolous investigative practices that are laden with bribery and corruption. The situation is even made worse because of less follow up at the level of the International Police Organization (INTERPOL). The Cameroonian 2010 law on cyber criminality attributes authority to investigative officers[62] to deal with cybercrimes. They are supposed to who abide by the rules of criminal procedure as captured by the 2005 Criminal Procedure Code.[63] But unfortunately, most of these officers collude with the perpetrator for personal gains. That is why most cybercrime cases are hardly prosecuted in Cameroon.[64] The phenomenon of hiding cyber criminals for financial gains through bribery and corruption is experienced today in many African countries as examined by Yushawu in 2020.[65] Most investigative officers prefer to take a bribe than to prosecute perpetrators before the law courts.

It is common to find cases where a suspected cybercriminal is arrested because of his suspicious financial activities by police and gendarme officers even without a complaint. The officers at times accompany the suspects to ATM machines to collect their own purported share of the illicit wealth. The officers at times force the suspects to transfer money from their mobile money accounts to their own accounts before letting them go. Accomplices of suspects commonly contribute bribes for the release of one of theirs. Some cybercriminals have made it a habit to put some officers on regular pay so that such officers can always shield them from any possible

[57] *Op.Cit*
[58] Some of the cases of impersonation have been detected during disciplinary board sessions by authorities of universities based in Molyko.
[59] Occultism describes various practices and beliefs related to the study of manipulation of supernatural forces. It involves a wide range of practices including divination, magic, alchemy, astrology and spiritualism.
[60] Although there are Human rights activists today in Cameroon who are advocating for the protection of the rights of lesbians, gays, bisexuals, transgender and queer people (LGBTQ).
[61] www.transparency.org (accessed on the 25th of April 2025)
[62] Section 52(1) of Law N° 2010/012 of 21 December 2010 relating to cybersecurity and cybercriminality in Cameroon
[63] Sections 59 and 60 of Law N°2005 of 27 July 2005 on the Criminal Procedure Code.
[64] Some of the bribes are taken most often from the suspects by force and coercion.
[65] www.bibliotekanauki.pl/PDF (accessed on the 23/04/2025)

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue V May 2025

eventuality. Furthermore, some suspects who fail to co-operate with some officers are often subjected to inhumane and denigrating treatment. These aspects raise legal problems under the due process of justice. Putting these ills together, erodes trust and confidence on Cameroonians to a greater extent both home and abroad.

Many opportunities to carry out legitimate e-commerce transactions in Cameroon with foreigners have been compromised. It may be noted that some Cameroonians residing abroad are notorious cybercrimes involved in scamming and phishing. This has caused some Cameroonians to face long term prison incarcerations in different countries abroad. Loss of trust and confidence in commercial transactions is experienced at all levels.[66] The impacts of cybercrimes on e-commerce have therefore discouraged many foreigners from engaging in e-commerce transactions with Cameroonians in general.

Arbitrary arrests and detentions due to e-commerce related cybercrimes

Arbitrary arrests and detentions on suspicions for e-commerce related cybercrimes without any complain is rampant in some regions of Cameroon like the Northwest and Southwest. Buea, Bamenda, Bambili and Limbe being notorious. The preamble of the Cameroon constitution[67] is clear that no person shall be arrested or detained except in the manner determined by law. The law that determines such arrest in Cameroon is the Criminal Procedure Code (CPC).[68] Contrary to the constitutional and procedural provisions on arrest and detention, most cybercrime suspects are arbitrarily arrested in violation of due process. Arrest in Cameroon ought to be done either under a warrant or under the *flagrante delicto procedure*[69] as prescribed by the CPC.

Due process is a fundamental aspect in legal proceedings that seeks to protect civil rights. Breaching same may lead to the nullification of an entire case.[70] In the e-commerce related cyber criminality cases of *The People v. Mbah Valery*,[71] and *the people of Cameroon v. Tamukum Fonjiyang Ferdinand & one other*,[72] the Court of First Instance Buea acquitted and discharged the accused persons. This was because of the violation of some procedural aspects of the CPC that included illegal arrests and detention.[73] The decision to discharge the accused persons went a long way to show the importance of protecting fundamental human rights.[74] It is therefore problematic when suspects are intercepted by the forces of law and order in violation of their constitutional and legal rights under the pretext of enforcing the law.

Illegal arrests and detention ought to be discouraged because it violates the fundamental principles of civil liberty enshrined in most international conventions and domestic laws. Article 9 of the International Covenant on Civil and Political Rights (ICCPR) 1966 prohibits arbitrary arrest and detention while article 6 of the African Charter on Human and People's Rights (ACHPR)1987 guarantees the right to liberty and clearly articulates that the deprivation of this freedom must be for reasons and conditions laid down by the law. These legal provisions are applicable in Cameroon pursuant to article 45 of the 1996 constitution as revised.[75]

Efforts are being made in Cameroon to curb the phenomenon of illegal arrests on suspicions for committing e-commerce related cybercrimes. The Southwest regional Branch of the National Human Rights Commission for example has been fighting against arbitrary arrest and detention because it is part of its mission to do so. The continuous arbitrary arrest of youths in the southwest region on the grounds of scamming has been seriously

[66] As noted by Rainer B. and Tyler Moore in 2012, most individuals who have been victims of cybercrimes in online commercial transactions end up never engaging in it again for fear of victimization while those who do not know about cybercrimes are more likely to engage in online commercial transactions.
[67] Law N° 96-6 of 18 January 1996 (as revised)
[68] Section 30 of Law N° 2005 of 27 July 2005 on the Criminal Procedure code.
[69] Section 31 ibid.
[70] See sections 3 and 8 of the CPC dealing with absolute and relative nullity. See also the decision of Lord Denning in the case of United Africa Company Limited (U.A.C) v. Macfoy dealing on nullity.
[71] CFIB/255/2010(Unreported).
[72] (2014) 2 SLR.
[73] The trial court held in the latter case that although the character of the accused persons was doubtful, they shall walk away from the court as free people.
[74] See ICCPR and the ACHPR.
[75] Article 45 of Law N° 96-6 of 18 January 1996 on the Cameroonian Constitution.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue V May 2025

criticized by the commission. It may be observed that the commission has intervened several times in cases of arbitrary arrests and detention in relation to alleged cybercrimes.[76]

The recent case of a youth[77] who was arrested in Buea in April 2025 for alleged e-commerce cybercrime related offences is under serious scrutiny by the commission. The victim who was returning home after following a football match was arrested, detained and tortured by the elements of the Police and Gendarmes. He was requested to pay for his release while purporting that he is a scammer. Since the victim could not provide the amount requested, he was forcefully taken to his home where an illegal search was conducted. Still unsatisfied, the officers led the victim to an ATM cash dispenser where he was forced to do a withdrawal for the officers' benefit. Meanwhile, the victim's younger brother who is a minor was detained in order to stop him from alerting others about the arrest of his brother.

It is alleged that since the victim could not do a withdrawal, he was forced by the officers to borrow part of the requested sum from his friends. They collected same before his release. The extorted amount was subsequently recovered by the Human Rights Commission while the case is still pending investigations. It may be recalled that a similar situation took place in 2024 along the Tiko-Douala highway where the same Human rights commission intervened. These are only a few examples. Many of such cases abound in Cameroon.

Economic impacts on e-commerce caused by cybercrimes

The growth of e-commerce related cybercrimes in Cameroon has led to financial losses and profits on individuals and corporate bodies. It has also led to diminished interest to engage in e-commerce transactions. This is because as examined by Billy Henson in 2011,[78] fears caused by cybercrimes due to victimization have a greater impact in cyberspace. Because cybercrimes are highly connected to e-commerce transactions in Cameroon, its adverse effects has led to a drop in demand for e-commerce services. This has invariably reduced turnover and output in businesses. Some financial losses due to e-commerce related cybercrimes may lead to bankruptcy. The amount of financial loses for instance as observed above was significant considering that Cameroon is still a developing nation. Such loses go a long way to distort the economy of the country and the smooth functioning of e-commerce transactions.

One of the purposes of e-commerce is to achieve fast turnover. With the proliferation of cybercrimes in Cameroon, there is a huge challenge because the demand for e-commerce services is dwindling. The ensuing consequences is that there are risks associated to high inflation,[79] money laundering and currency counterfeiting.

CONCLUSION

This article has examined the impacts of Cybercrimes related offences on e-commerce transactions in Cameroon. It reveals that the high rate of cybercrimes related to e-commerce transactions in some major cities of Cameroon are mostly perpetrated by youths with the number of potential offenders on the rise. The findings of this research reveals that e-commerce related cybercrimes in Cameroon have led to loss of trust and confidence with arbitrary arrests and detentions in violation of due process. It observed that most suspect are hardly brough before the competent law courts because police officers prefer to take bribes and set the suspects free. The findings further show that cybercrimes in e-commerce related transactions have tarnished the reputation of Cameroonians at home and abroad with some foreigners losing interest to conduct e-commerce transactions with most Cameroonians.

It is therefore recommended that legal, technological, social and economic reforms should be instituted in Cameroon to resolve the issues identified. That legislation in Cameroon on cyber criminality and e-commerce should be improved upon by specifically addressing the procedural rules to follow at the investigative and litigation stages on cases of e-commerce related cybercrimes. That the law should empower the National

[76] www.the guardianpostcameroon.com/post/6456/en (accessed on the 27th of April 2025)
[77] The name is still withheld because the case is still under investigation.
[78] www. journals.sagepub.com (accessed on 25/04/2025)
[79] It can be observed that the prices of basic commodities in Buea is high as compared to other cities in cameroon because of illegal wealth that is used in Buea by mostly youths who are scammers.

Financial investigation agency (NFIA)[80] and the National Agency for information and communication technologies (NAICT)[81] to prosecute cases of e-commerce related cybercrimes. That the forces of law and order should be adequately trained on arrest procedures and detention in cases of cyber criminality. The officers should also be provided with incentives after any successful e-commerce related cybercrime prosecutions. On the other hand, serious sanctions should be applied in cases of corruption and bribery in e-commerce related cybercrimes. That the minimum wage level and the salaries of Cameroonians should be improved while creating new jobs to absorb idle youths. That Schools should introduce cybersecurity and e-commerce lessons in their curricula from the elementary level. That a proper home address system and social security numbers be instituted in Cameroon.

REFERENCES

1. Brayan A. Garner, Black's Law Dictionary: Minnesota, West Group, (1999) P. 392.
2. Chris H., et al, Criminology: Oxford, Oxford University Press, (2005) p.
3. Griffin, Salade E., Rackley, Casey C. ''Vishing''. Proceedings of the 5th annual conference of information security curriculum development. (2008).
4. Haung L., Orbach B., ''Con men and their enablers: The anatomy of confidence games'' Social Science international Quarterly Vol 4(2018)
5. Payne, Brian K., The Handbook of International Cybercrime and Cyber evidence: London, Palgrave Macmillian, (2020).
6. Wartiovaara, M. Rationality, ''REMM, and Individual Value Creation.'' Journal of business Ethics, Vol 98, (2011).
7. Jansson, K.; von Solms, R. ''Phishing for phishing awareness.''Behaviour & Information Technology. Vol 32 No 6 (2011).

[80] Popularly Known in Cameroon by its French acronym as ANIF
[81]Popularly Known in Cameroon by its French acronym as ANTIC