The Protection Of E-Banking Services Against Cybercrimes In Cameroon: Prospects And Challenges

Nkambeh Allen Ghaseh
Ph.D. Researcher in the Department of English Law, Faculty of Law and Political Science University of Dschang, P.O. Box 66 Dschang, Cameroon
Email: allenghaseh@gmail.com

***Abstract*— This article seeks to examine the extent to which users of e-banking services are protected in Cameroon. Over the past decades financial transactions have gradually emerged from traditional methods to modern forms of banking. The Information and Communication Technology (ICT) has transformed the banking system into a digital arena. With e-banking, customers can access their bank accounts, transfer funds, pay bills, and check their accounts balances. Banks serve as the backbone of every modern economy and should be protected. The development of e-banking in the 1980s with the aid of ICT has rendered banks and their customers vulnerable to cybercrimes. As an effort to combat cybercrimes and ensure cyber security in Cameroon, the 2010 Cyber Law provides both substantive and procedural rules. It is rather unfortunate that, the measures put in place to ensure cyber security and protect bank customers against cybercrimes are to a greater extent ineffective. The main objective of this article is to determine the protection accorded to banks and their customers against cybercrimes. The method adopted in the course of this work is doctrinal wherein, both primary and secondary sources of data were collected. The findings reveal among others that, the measures put in place to combat cybercrimes within the banking sphere in Cameroon are not effective. There is lack of explicit definitions for cyber offences. Most of the offences provided by the 2010 Cyber Law are vague and ambiguous. We therefore recommend that, the 2010 Cyber Law should be amended to address the current issues of ICT. This amendment should include explicit definitions for the different forms of cybercrimes with severe sanctions. Banks are advised to put in place effective monitoring machineries to mitigate cybercrimes.**

Keywords—E-banking; Protection; Cybercrimes, Prospects, Challenges.

1. Introduction

The introduction of Information and Communication Technology (ICT) has brought about development in our society today. The use of technological devices such as computer software, the internet and mobile phones have helped to facilitate communication networks. These devices ensure a fast exchange of information.[1] The exchange of information has enabled corporations, government and personal information to be available to the public at the global level. Banking activities have evolved from the traditional forms of banking to the modern forms of banking with the introduction of ICT.[2] Electronic banking (e-banking) which started in the early 1980s have brought about some changes in the banking industry.[3] It is a form of banking in which the customer conducts transactions electronically via the internet. That is, it is an

[1] Gercke Marko, (2009), *Understanding Cybercrime: A Guide for Developing Countries*, Geneva, International Telecommunication Union (ITU), Telecommunication Development Centre, P. 12.

[2] Aazib Afraz T. & Geetha R., (2024), "E-banking: Opportunities and Challenges from Customer's Perspective", Vol. 4, *QUBAHAN ACADEMIC JOURNAL*, P. 354.

[3] Wangui Phelista N., (2019), "Investigating extent to which Cybercrime Influences Performance of Commercial Banks in kenya", Vol. 7, *International Journal of Economics, Commerce and Management*, United Kingdom, P. 490

arrangement between a bank or a financial institution and its customers that enables encrypted transactions over the internet. It is also the use of electronic methods to transfer money directly from one account to another.[4] Electronic banking offers customers the convenience of accessing banking services 24/7 at the comfort of their homes or offices. Customers can access their bank accounts, transfer funds, pay bills, check their accounts balances and also access their transaction history online, without actually visiting a physical bank branch.[5] The emergence of ICT has an impact on almost every area of human activities. These impacts have been felt in the banking sector. The innovation brought by ICT has also increased the level of risks within the banking institutions such as phishing, unauthorized access, fraudulent transactions, hacking, online theft of user ID/username, passwords, virus attacks, pharming and money laundering amongst others.[6] Cybercrime evolved in the 1980s where a basic computer virus kicked off the evolution of cyber-attacks.[7]

The emergence of ICT pose security risk to banks and their customers. As a result of the security threats posed by ICT, banks and their customers are in a state of constant fear of losing their financial credentials to cybercriminals who are experts of this new system of technology.[8] Cyber security threats have rendered banks and their customers vulnerable to data risk and other related cybercrimes. The measures put in place to ensure cyber security and to protect bank and its customers against cybercrime are ineffective and insufficient in responding to the uprising cybercrimes in Cameroon. Banks and their customers are still exposed to cyber threats despite the existence of both national and international laws to combat cybercrimes. The fight against cybercrimes in the banking sector remains a call for concern. This article therefore, calls for robust legal and institutional measures to address the growing cyber perpetrations.

2. Legal Framework for Data Protection in Cameroon

Cameroon has made an expressed intention to combat cybercrimes across the territory. This effort can be deduced from the establishment of legal instruments to enhance data protection in Cameroon. The principal norm regulating cybercrimes in Cameroon is Law No. 2010/012 of 21 December 2010 relating to Cyber Security and Cyber Criminality in Cameroon.[9] More recently, Cameroon has intensified its willingness to combat cybercrimes by adopting Law No. 2024/017 of 23 December 2024 on Personal Data Protection in Cameroon. The Law on Electronic Commerce in Cameroon also regulates e-banking services in Cameroon. These legal instruments are examined below.

[4] Awah Ambe H., (2022), "The Protection of Users of E-banking Services in Cameroon: A Legal Approach", Vol. 4, *Journal of Banking and Insurance Law*, P. 27.
[5] Vidhya Jolly, (2016), "The Influence of Internet Banking and cost Savings for Banks' Customers", Nepal, *International Journal of Social Sciences and Management*, Vol. 3, issue 3, P. 163.
[6] https://yacenter.org>internet-banking visited on the 28th of April 2025.
[7] Batra Kumar N. & Gulat Parul, (2022), "Cyber-Attacks on Banking Institutions in India: Safety and Preventive Measures", Vol. 2, *International Journal of Innovations & Research Analysis (IJIRA)*, P. 21.
[8] Wangui Phelista N., (2019), Op. Cit. P. 491
[9] Hereinafter referred to as the 2010 Cyber Law

2.1. The Law on Cyber Security and Cyber Criminality in Cameroon

The 2010 cyber law governs the security framework of electronic communication networks and information systems in Cameroon. It defines and punishes offences related to the use of information and communication technologies in Cameroon. [10] The primary objective of the Cameroonian Cyber Law is to build trust in electronic communication networks and information systems; to establish the legal regime for digital evidence, security, cryptography and electronic certification activities; protect basic human rights, in particular the right to human dignity, honour and respect of privacy, as well as the legitimate interests of corporate bodies. The 2010 Cyber Law also made provisions for the protection of electronic communication networks, information systems and personal privacy.

The protection of electronic communication networks as provided under section 24 of the Cyber Law states that, electronic communication networks operators and electronic communication service providers must take all the necessary technical and administrative measures to guarantee the security of the services provided. To that end, they shall be bound to inform users about; the risks of using their networks, the specific risks of security violation, notably the denial of services distributed, abnormal rerouting, traffic points, traffic and unusual ports, passive and active listening, intrusion and any other risk, the existence of techniques to ensure the security of their communications. [11] Providers of e-banking services are required to take measures to ensure the security of the electronic communication network. The Cameroonian Cyber Law can be presumed to have provided for the protection of bank customers with regards to electronic services (e-banking) offered by e-bankers to their customers.

2.1.1. The Protection of Privacy under the 2010 Cyber Law

The 2010 Cameroonian Cyber Law gives priority for the protection of privacy. It states that; every individual shall have the right to the protection of their privacy. Judges may take any protective measures notably, sequestration or seizure to avoid or end the invasion of privacy.[12] It equally gives operators of electronic communication and networks information systems, the duty to ensure confidentiality of information channelled through electronic communication and information systems networks,[13] including traffic data.[14] By virtue of section 44 of the 2010 Cyber Law, it shall be forbidden for any natural person or corporate

[10] Ibid Section 1.

[11] The Cyber Law equally stipulates that network operators and electronic communication service providers shall be bound to conserve traffic connection data for a period of 10 (ten) years (see Section 25(1) of the 2010 Cyber Law in Cameroon). Where the Network operators and electronic communication service providers undermine the individual liberties of users, they shall be liable with regards to their duty to conserve traffic connection data for a period of 10 (ten) years (Section 25(3) of the 2010 Cyber Law).

[12] Section 41 of the 2010 Cyber Law

[13] Ibid section 41

[14] Traffic data refers to any information (data) processed for the purpose of conveyance of a communication on an electronic communication network or for the billing in respect of that communication and includes data relating to the routing, duration or time of a communication.

body to listen, intercept and store communications and the traffic data related thereto, or to subject them to any other means of interception or monitoring without the consent of the users concerned, but it's save where such a person is so authorised legally.[15] Banks have the duty to keep confidential information of their customers which are obtained for business purposes.[16] Banks that provide electronic services to customers must ensure that all the information relating to customers' bank account is kept secret and protected from cybercriminals.

2.1.2. International Cooperation for the Fight against Cybercrime as Enshrined in the 2010 Cyber Law

The 2010 Cyber Law provides for international cooperation and mutual judicial assistance in the fight against Cybercrimes in Cameroon. In this light, Cameroon and other nations can work together in many ways to combat cybercrime all over the world.[17] This international cooperation as provided in the 2010 Cyber Law relates to international judicial cooperation and international mutual assistance.[18] International Cooperation is needed in order to combat the prevailing cybercrimes in the world today.[19] Cameroonian Certification Authorities in carrying out their duties may, under the control of the Agency, conclude conventions with foreign Certification Authorities.[20] There is a need for mutual judicial cooperation between Cameroon and other countries.[21]

2.1.3. Sanctions for Cybercrimes under the 2010 Cyber Law

The 2010 Cyber Law makes provisions for different offences and the accompanying sanctions. According to section 61(1) of the Cyber Law, agency personnel and experts of corporate bodies in charge of security audits who without any authorization, disclose confidential information they are privy to on the occasion of a security audit shall be punished with imprisonment as from three (03) months to three (03) years and a fine as from 20,000 (twenty thousand) to 100,000 (one hundred) CFA francs. In this light, banks have the duty to conserve the information they obtain from their customers and where such information is disclosed without authorisation or request from customers or law enforcement agents, they will be liable as per the 2010 Cyber Law. The 2010 Cyber Law provides sanctions for corporate bodies for acts that violate the security or the rules of confidentiality of the

[15] However, technical storage prior to transmission of any communication shall be authorized for electronic communications' networks and information systems operators, without prejudice to the principle of confidentiality. See Section 44(2) of the Cyber Law.

[16] This relates to the aspect of bank secrecy which requires both the bank and its customers to keep privacy with regards to any potential information (confidential information) which they might obtain in the course of their transactions or dealings.

[17] Kwei Haliday N. et al, (2023), "Delineating International Cooperation in the Fight against Cybercrime in Cameroon", Vol. 49, *International Journal of Computer (IJC)*, P. 32

[18] Part IV of the 2010 Cyber Law

[19] Because of the vast nature of ICT, information is made available across the national globe in this light; cybercrimes are also trans-border crimes where an offender residing in one country can launch a cyber-attack on an individual or corporate body residing in another country. Therefore, there is a need for Cameroon to cooperate with other countries by signing conventions aimed to assist one another in the fight against Cybercrimes.

[20] Section 90(1) of the 2010 Cameroonian Cyber Law

[21] Ibid, Section 91(1)

services offered. Corporate bodies are criminally liable for offences committed on their account by their management structures. [22] The criminal liability of banks shall not preclude that of natural persons [23] who commit such offences nor are accomplices.[24]

The penalties to be meted out on defaulting corporate bodies as provided by the 2010 Cyber Law shall be fines as from 5 000 000 (five million) to 50 000 000 (fifty million) CFA francs.[25] A bank providing electronic services to customers and fails to maintain the security measures as prescribed under this law is subject to the above stated sanctions. Other corporate sanctions for cybercrimes are provided in Section 64(4) of the 2010 Cyber Law.

The above Law also sanctions whoever uses an information system or a counterfeit communication network to falsify payment, credit or cash withdrawal card or uses or attempts to use, in full knowledge of the facts, a counterfeit or falsified payment, credit or withdrawal card shall be punished with imprisonment as from 2 to 10 years and a fine from 25,000,000 to 50,000,000 CFA francs or with both such imprisonment and fine. [26] It further states that whoever deliberately accepts to receive electronic communications payment using a forged or falsified payment, credit or cash withdrawal card shall be punished with the same sanctions.[27]

2.2. The Law on Personal Data Protection in Cameroon

Personal data protection in Cameroon is governed by Law No 2024/017 of 23 December 2024. This recent law on personal data protection in Cameroon has equally shown the effort of the Cameroonian government to mitigate cybercrimes in Cameroon by enhancing personal data protection within the country. This law aims to guarantee the fundamental rights and freedoms of individuals with regards to processing of personal data, irrespective of the type of data, the processing method and the persons responsible.[28] The 2024 law on personal data protection in Cameroon requires anyone processing personal data to ensure its confidentiality on digital communication networks or any other medium.[29]

The law on personal data protection in Cameroon protects banking activities by prohibiting the processing of personal data in connection to banking transactions without the prior consent of the competent public authorities and bodies. [30] This new law on personal data protection has made provisions for administrative, civil and penal sanctions.

2.2.1. Administrative Sanctions

These sanctions are melted where the personal data protection authority realises that the processor or controller has failed to comply with

[22] Ibid, Section 61(1)
[23] The management directors of the bank who fail in their duty to ensure the security of potential or confidential information belonging to their customers and thereby subjecting such information to cyber threats, shall be criminally liable as provided in the Cameroonian Cyber Law.
[24] Section 64(2) of the Cyber Law
[25] Ibid, Section 64(3)
[26] Ibid, Section 73 (1).
[27] Ibid, Section 73 (2).
[28] See Section 1 of Law No. 2024/017 of 23 December, 2024 on Personal Data protection in Cameroon.
[29] Ibid, Section 7.
[30] Ibid Section 48 (2).

the obligations. In this light, the authority concern shall give the processor or controller formal notice to comply within 10 days from the date of receiving the notice.[31] If after 10 days, the processor do not comply then the Personal Data Protection Authority shall proceed to issue an injunction in order to ensure compliance of processing personal data. It is also subject to a fine of 100,000 CFA francs per day for any delay after the stated 10 days.[32] If the processor fails to comply, the authority may suspend the activity for which authorisation was granted for or withdraw the authorisation or prohibit the party concern from carrying out any activity that involves the processing of personal data.[33] It furthers stipulate that whoever engages in the processing of personal data without prior authorisation shall be punished with a fine as from 5,000,000 to 50,000,000 CFA francs.[34]

2.2.2. Civil Sanctions

Where the rights to personal data are seriously infringed, the data subject may petition a competent court ruling under the emergency procedure, to order any measure that is necessary to protect his/her rights. The data subject may equally apply to the competent court for compensation to be made for such an infringement.[35] Bank customers whose data rights have been breached by the bank can petition the competent court for such rights to be maintained and where necessary compensation will be granted.

2.2.3. Penal Sanctions

The new law on personal protection also provide for penal sanctions. It states that whoever collects or processes personal data by fraudulent, unfair or unlawful means shall be punished with an imprisonment term of two to five years or a fine as from 200,000 to 5,000,000 CFA francs, or with both such imprisonment and fine.[36] It also punishes anyone who discloses personal data to a third party without the consent of the person involved with an imprisonment term as from six months to two years or a fine of from 200,000 to 5,000,000 CFA francs or both such imprisonment and fine.[37] This law equally sanctions legal persons that are criminally liable with a fine as from 50,000,000 to 1,000,000,000 CFA francs.[38] Banks by virtue of Section 71 of the 2024 Law on personal data protection in Cameroon can be criminally liable for data breach and can therefore be made to pay the stated fine.

The Law on Personal Data Protection in Cameroon has made provisions for the protection of personal data. However, this law do not provide measures that are necessary to preserve or keep personal data of individuals safe from cyber perpetrators. Cyber insecurity remains a major call for concern in Cameroon today due to the continuous cyber intrusions committed. Providing individuals with safeguarding measures to protect their personal data from cybercriminals

[31] See Section 54 (1) of the 2024 Personal Data Protection Law in Cameroon.
[32] Ibid, Section 54 (2).
[33] Ibid, Section 54 (3).
[34] Ibid, Section 55.
[35] Ibid, Section 62.
[36] Ibid, Section 63 (1).
[37] Ibid, Section 68 (1).
[38] Ibid, Section 71.

is prerequisite for the fight against cybercrimes within the banking industry in particular and other e-commerce transactions in general.

2.3. The Law on Electronic Commerce in Cameroon

Electronic Banking is one of the electronic commercial activities in Cameroon that greatly contributes to economic growth and development of the country. Electronic commerce in Cameroon is regulated by Law. No. 2010/021 of 21 December 2010. It covers electronic means of payment. [39] Electronic commerce is a commercial activity in which a person uses electronic means to supply or ensure the supply of goods or/and services. Electronic commercial transactions are often done using the electronic networks which enable both customers and their suppliers to transact over long distances. E-commerce requires an electronic payment system to facilitate payment transactions between parties.[40] The electronic payment system exposes the bank and its customers to cyber risks.

The law on e-commerce requires every service provider to store or keep data relating to any commercial transaction carried out by electronic means in accordance with the laws and regulations in force. [41] This is to avoid the disclosure of important or confidential information belonging to customers.[42] In case of any loss or theft, the 2010 law on e-commerce in Cameroon states that *"the holder of the electronic means of payment shall notify the issuer of the loss or theft of the means or instruments used to operate it, as well as any fraudulent use it is aware of."*[43] It also provides in Section 28 (2) that the issuer of an electronic means of payment shall include the appropriate means for such notification in the contract.[44]

3. Forms of Cybercrimes

They are different types of cybercrimes that affect e-banking. These crimes have drastically increased as digital technology keeps on evolving. It becomes more complex to maintain a secure digital world. Cybercrime in the banking sector is a criminal activity that involves the use of computers and the internet.[45] The target of cybercriminals since the 1980s has been directed towards financial institutions. The main objective here is to steal data, disrupt services and gain unauthorised access. Some of

[39] This refers to the means enabling its holder to carry out distance payment through telecommunications networks. See Section 2 of Law No. 2010/021 of 21st December 2010 on Electronic Commerce in Cameroon.

[40] Ibid Section 27 states that "Payment operations may be carried out in public services electronically under the conditions lay down by the laws and regulations in force.

[41] Ibid Section 32.

[42] The 2010 Law on e-commerce therefore protects bank customer's data; by obliging banks (service provider) to store or keep the data they obtain from customers in a manner that comply with the established rules and regulations.

[43] Section 28 (1) of the Law on E-commerce in Cameroon

[44] According to Section 29 (1) of the 2010 law on E-commerce in Cameroon in cases of fraud notwithstanding the holder of the electronic means of payment shall:

-until notifies the issuer, assume responsibility for the loss or theft of the means of payment or the fraudulent use thereof by a third party;

-be released from all responsibility for the use of the electronic means of payment after notifying the issuer. Section 29 (2) provides that *"the use of the electronic means of payment without presentation of the said means if payment and identification by electronic means shall not commit its holders."*

[45] https://www.63sats.com (accessed on the 5th April 2024)

these cybercrimes which have a negative impact on e-banking services are discussed below.

3.1. Phishing

It is a trick used to get potential information from bank customers. It involves the sharing of secret information like; usernames, credit cards details or passwords. This crime occurs when someone pretends to be another person via emails or messages which entice people to think that it is safer to share personal information.[46] These emails or messages are often 'too good to be true' enticing people to part with personal details, information, or money, or to click on links or open attachments [47] are a worrying and growing trend. Some of the emails or messages are convincingly made to target the vulnerable.[48]

3.2. Samali Attack

This type of cybercrime is prevalent within financial institutions and it is aimed to commit financial crimes. Samali attack is a fraudulent activity which targets financial systems specifically. For instance, a bank employee inserts a program into the financial systems, which deducts a small amount of money from every customer's account and no account holder will notice this unauthorised debit. The bank employee will make a monthly salary from this deduction. The hacker simply slices away small sums of money from multiple accounts.[49] This fraudulent act can damage the bank's reputation in the eyes of its potential customers and amount to increase cost on the bank (payment of damages to victims).[50]

3.3. Ponzi-Schemes

This is an investment scam that pays early investors with money taken from later investors to create an illusion that there is a big profit. Ponzi schemes entice investors with a high rate of return with very little investment risks presented. It is an investment scheme promising high profit. This type of scam often relies on word-of-mouth, as new investors hear about the big returns earned by early investors.[51]

3.4. Hacking

This is a type of crime which involves unauthorised intrusion into computer systems, networks or software.[52] This offence is committed using different tools and tricks such as breaking in, stealing or changing data, stopping services or the exploitation of weaknesses in systems for

[46] Kumudha S. & Aswathy R., (2018), "A Critical Analysis of Cyber Phishing and its Impact on Banking Sector", Vol. 119, *International Journal of Pure and Applied Mathematics*, P. 1558.

[47] Often accompanied by giving a sense of urgency, most of the messages sent often appear to be handled within a limited time. It does not give room for doubts or contemplation of such emails or messages.

[48] Jurjen Jansen & Rutger Leukfeldt, (2016), Phishing and Malware Attacks on Online Banking Customers in Netherlands: A Qualitative Analysis of Factors Leading to Victimization" Vol. 10, *International Journal of Cyber Criminology*, P. 83.

[49] LINEARSTACK (2023), "Preventing Data Diddling and Samali Attacks", available on www.linearstack.com (accessed on the 13th April 2025)

[50] Yuniawati Y. et al., (2021), "Factors Detecting Employee Fraud: A Study Among Private Companies in Jarkarta", Vol. 570, *Proceedings of the International Conference on Economics, Business, Social and Humanities*, P. 503.

[51] https://www.investopedia.com, (accesses on the 14th April 2025)

[52] Vijay Ramalingam, (2019), "Impact of Hacking on Cyber Security", Vol. 6, *Journal of Emerging Technologies and Innovative Research*, P. 132.

malicious reasons.[53] By creating fake accounts or tricking people, cybercriminals get personal/sensitive information such as login credentials, banking details, or take over someone's social media account.

3.5. Pharming

This is another form of cybercrime in which the attackers use a technique that manipulates the Domain Name System (DNS) aimed to redirect a user's legitimate request to a fraudulent website without their knowledge. The pharming technique is based on compromising the DNS server or the user's local host file, thereby causing the DNS queries to resolve to the attacker's IP address instead of a legitimate one.[54] This fraudulent site is designed to capture sensitive information such as; usernames, passwords including credit card details. Most often these sites appear more legit and many users do not give a second thought when accessing such websites.

3.6. ATMs Skimming and Point of Sale Crimes

Automated Teller Machines skimming occur when hackers use devices to steal information from cards at ATMs. This is done by placing a sneaky device on the machine which secretly takes the card information and PIN codes when someone uses it.[55] This can be done by stealing the credit/debit card information during a legitimate transaction using a skimming device. Attackers are able to cash out an ATM by using malware to infect and manipulate the machine.

3.7. Electronic Money Laundering

This is the use of the internet by cybercriminals to conceal funds which are illegally obtained. This is done by funnelling the money via various banks and financial transactions making the funds appear legitimate. That is, the proceeds of these scams are transmitted electronically through financial institutions for non-traceability. Money laundering has a negative impact on e-banking users in that the money may have been funds stolen or transferred from their accounts.[56]

3.8. Viruses

Viruses are infectious programs which connect to other pieces of software or programs and replicate once the software begins to run.[57] That is, a computer virus is a program that makes copies of itself. Just like human viruses need a body to replicate, so too does a computer virus need a computer to replicate. Viruses often

[53] This exploitation of weaknesses is also known as "Penetration Testing". This is a form of ethical hacking which is a legal hacking that is bound by the rules, if the rules are denied, then the hacker must pay higher price in the form of penalties which can be monetary or otherwise.

[54] Ranny Caroline & Miniawati Tina V.B., (2025), "Analysis of Pharming in Cyber Crime and its Impact on Customer Trust (Case Study on Bank BRI Customer Bandar Lampung Regional Office)", Vol. 3, *International journal of Accounting, Management, Economics and Social Sciences*, P. 262.

[55] Cyber Crime in the Banking Sector: Strategies to Mitigate the Impact of Cyber Attacks, available on https://www.63sats.com (accessed on the 25th April 2025).

[56] Djieufack Roland and Awah Ambe Harvey, (2019), *Users of E-Banking within the CEMAC Zone: The Cameroonian Experience*. Éditions Universitaires Européennes, P. 171.

[57] Kaira Milani F., (2023) "Banking Malware Attacks and Security Solutions Review", Vol. 1, *Jurnal Penelitian Sistem Informasi (JPSI)*, P. 55

penetrate into computers by hiding a program or file, such as a photograph.[58]

4. Effects of Cybercrimes on E-banking

The introduction of ICT has undoubtedly reshaped the banking atmosphere via electronic services. However, ICT has equally brought about cybercrimes. These cybercrimes have devastating consequences on e-banking services. Some of these effects include; financial loss, reputational risk and operation risk among others.

4.1. Financial Loss

Banks are constantly faced with threats from cybercriminals in today's digital world. Since banks use information technology and online platforms to provide financial services to customers, it becomes easier for hackers to target banks. According to the Cyber security Ventures Report, cyber-attack on banks in between 2014 to 2019 has caused an average loss of 18 million dollars per incident.[59] In 2021 cyber-attack on banks were estimated to have amounted to a financial loss of 6 trillion dollars worldwide.[60]

In the past two decades, nearly one-fifth of reported cyber incidents affected the global financial sector. This, according to the International Monetary Fund (IMF) report of 2020 caused 12 billion dollars to financial institutions.[61] According to this report, banks are particularly targeted and the losses recorded are likely much higher as compared to indirect losses and reputational damage.[62] The IMF's report calls on financial institutions to amplify their cyber security capacity via measures such as stress testing and information-sharing arrangements, among others recommendations. The IMF also urges state authorities to develop appropriate and adequate cyber security strategies that are accompanied by regulatory frameworks.[63]

4.2. Reputational Risk

Reputational risk management in banks covers the topic of the risk of loss of reputation. Unlike other risks that banks have to manage such as credit, market, operational, liquidity, etc., reputational risk is intangible and hard to measure. With the development of ICT financial institutions including banks are exposed to reputational risks resulting from negative stakeholder opinion or the negative publicity made on social media by cybercriminals which has an adverse impact on the bank's current or projected financial conditions and resilience.[64]

4.3. Operational Risk

Operational risks remain critical to banks as malicious cybercrime activities evolve and

[58] Shea John M., (2013), *Combating Computer Viruses*, 1st Edition, Gareth Stevens, New York, USA, P. 6

[59] See "Cyber Crime in Banking Sector: Strategies to Mitigate Cyber Attacks" available on https://63SATS.com (accessed on the 23rd of March 2025)

[60] Ibid

[61] The IMF's Global Financial Stability Report, available on https://www.weforum.org (accessed on the 30th of March 2025).

[62] The report also reiterates that "cyber incidents are a key operational risk that could threaten financial institutions' operational resilience and adversely affect overall macro-financial stability." The report added that "while cyber incidents thus far have not been systemic, on-going rapid digital transformation and technological innovation and the heightened global geopolitical tensions exacerbates the risk".

[63] The Report states that "with the global financial system facing significant and growing cyber risks, policy and governance frameworks to mitigate the risks must keep pace."

[64] https://www.risk-officer.com ((accessed on the 16th of April 2025)

become more sophisticated, as banks adopt new technologies. In an increasingly digital world, banks are vulnerable to cyber-attacks which can compromise customers' data, disrupt operations, and erode trust.[65] With the rapid advancement of hacking techniques, including ransom ware attacks and data breaches. Cyber-security remains a top concern. To mitigate the risk of cyber incidents, banks must invest in robust cyber security measures, including advanced threat detection systems, employee training programs, and continuous monitoring. According to the 2023 Annual Survey of Community Banks conducted by the Conference of State Bank Supervisors and state financial regulators, cyber security continues to be a top internal risk priority for community banks.[66] When a bank's reputation is attacked on social media this can cause the bank a serious financial loss. Reputational risk may cause customers to be reluctant to continue using the products or services of the bank.[67]

4.4. Infringement of Confidential Information

Cybercrime breaches the bank's duty of secrecy. Banks are under a duty to ensure that all the information gotten from customers in the course of their transactions is kept secret.[68] Bank customers trust their banks with their data. This includes some of the most sensitive personal information and financial data, like social security numbers, passwords, logins, PIN numbers, and bank account numbers.[69] Most of the financial losses that banks and their customers incur from cybercrimes results from infringement of confidential information.

While the costs are unfathomable, cyber-attacks are particularly devastating because their effects are seldom known immediately. At times it takes victim organisations months just to recognize that an attack took place.[70] The difficulties encountered by banks to quickly detect cybercrimes, gives hackers an eternity to infect computers, servers, and networks. When this happens, hackers can easily have access to the bank's confidential information.

4.5. Legal Sanctions

Banks can be fined by regulatory authorities for failing to comply with cyber security regulations aim to protect customers' data, or report breaches promptly. Banks can be issued lawsuits by customers, partners, and employees for damages resulting from data

[65] Okpa Martins M., (2022), "An Assessment of Cyber Crime in Commercial Banks in Calabar Metropolis, Vol. 11, *Ibom Journal of Social Issues*, P. 24.

[66] Nearly 92% of respondents cited cyber security as an either "extremely important" or "very important" risk priority. Technological advancement requires bank managers to continuously improve cyber security and other internal controls to create operational resilience and mitigate the risk that their bank will suffer a significant service disruption.

[67] https://www.hkma.gov.hk (accessed on the 10th of April 2025)

[68] This duty extends even when the banking contract has come to an end. However, there are cases where the bank can disclose customers' information without being liable. For instance, where the law requires the bank to disclose, where the disclosure is to defend the bank's reputation by giving evidence in court.

[69] https://www.reviewtrackers.com/…/bank-reputation-risk , (accessed on the 16th of April 2025)

[70] According to an IBM report, the average breach takes 212 days to detect and another 75 days to contain.

breaches. [71] Also, cybercriminals can be prosecuted under laws and regulations that govern banking activities and online transactions.[72]

5. Challenges and Measures in Combating Cybercrimes

Despite the existence of legal rules to combat cybercrimes in Cameroon and even across the globe, e-banking services are still faced with cyber insecurity. The challenges in combating cybercrimes remain enormous. To respond to these challenges, certain measures are recommended to combat cybercrimes.

5.1. Challenges in Combating Cybercrimes

As earlier reiterated, the banking profession is currently faced with cyber insecurity. Banks have made advancement in the fight against cybercrimes. Despite these efforts by banks and even governments, the banks and their customers are still faced with cyber-threats. The challenges faced in the fight against cybercrimes include the following.

5.1.1. Legal Challenges

The evolution of ICT allows the storage and transmission of data on all types of electronic devices. [73] This creates several cybercrimes related to compromising the integrity, availability, or confidentiality of communications and data system. One of the main challenges in the fight against cybercrimes is the limited legislation on ICT. The sanctions provided for cybercriminals are less severe as compared to the financial and reputational loss which banks and their customers undergo in the hands of cybercriminals. Given the fact that technology is changing day by day, the 2010 cyber law do not identify all the cybercrimes as new cybercrimes keep evolving. Since a good number of these crimes remain unknown to the Cameroonian legislator,[74] there is a need to revise the 2010 cyber law so as to clearly define these cybercrimes and make provisions for severe punishments with respect to the gravity of such crimes.[75] There are no uniform international legal rules to sanction cybercrimes amongst states. This makes it more difficult to prosecute cybercrimes where offenders are from different states. The complexities that surrounds the acquisition of digital evidence can be resolved if states via conventions jointly unify legal sanctions against cybercrimes. The recent adoption of the United Nations convention on cybercrimes is hoped to fill in the gap left by local legislations.

5.1.2. The Complex Nature of Cyberspace

Cyberspace refers to the virtual environment created by interlocking networks of computers and electronic systems. That is, it is that realm in which online communications, data

[71] Artificial Intelligence Overview, (accessed on the 16th of April 2025)

[72] These cyber sanctions are provided principally by the 2010 Cyber Law in Cameroon.

[73] Viraja V.K. & Pradnya Purandare, (2020), "A Qualitative Research on the Impact and Challenges of Cybercrimes", *Journal of Physics: Conference Series*, P. 1.

[74] This is with regards to the 2010 cyber law in Cameroon.

[75] The inadequacy of legal texts and less severe sanctions for cybercrimes are some of the challenges for the fight against cybercrimes.

exchange, and digital interactions take place.[76] The nature of cyberspace[77] is dynamic. That is, cyberspace is constantly changing as technology also advances and new actors or users equally emerge. These dynamics in technology makes cyberspace undefined and exponential as compared to the physical world which is static and well defined. Another complex element of cyberspace is its global nature. Cyberspace does not have any limited national boundaries. This makes information to be available across national territories. The widespread of information technology makes it more difficult for states to implement their cyber laws and regulations across different jurisdictions.

5.1.3. Difficulties in Identifying Cybercriminals

Cyber-activities operate under an opened network. That is, the vast nature of cyberspace which involve users all over the world. The open nature of cyberspace makes it difficult for investigating officers to identify cyber perpetrators. This is coupled with the difficulties in proving cybercrimes and acquisition of digital evidence. The primary objective of if not all but many cyber laws established by states are to sanction cybercriminals and to enhance cyber security.[78]

5.1.4. Lack of Monitoring Machineries

Many financial institutions, governments and other organisations that are faced with cyber insecurity lack preventive and recovery tools for cybercrimes. Cybercrime often requires the use of specialised tools and software to collect, preserve, and analyse digital evidence. These tools can be used to identify suspects, track the activities of cybercriminals and assemble admissible evidence for prosecution. Some of these vital tools include; network analysis tools, passwords recovery tools, digital forensics software, malware analysis tools and social media analysis tools.

5.1.5. The Emergence of Artificial Intelligence (AI)

The introduction of artificial intelligence (AI) has unarguably improved the digital world by making information easier to access. Artificial intelligence is a set of digital technologies that allow machines to perform tasks that are usually associated with human intelligence. However, AI is technology that enables computers and machines to simulate human learning, comprehension, problem solving, decision making, creativity and autonomy. [79] The emergency of AI which could be regarded as an important digital device to help mitigate cybercrime within the banking sector has rather facilitated cyber operations. [80] Generative

[76] See https://www.sentinelone.com , (accessed on the 12th of April 2025).

[77] The term cyberspace was introduced in the early 1980s by American science fiction novelist called William Gibson in his work entitled “Neuromancer”.

[78] Therefore, difficulties in identifying cybercrimes also denote cyber injustice. If offenders are unable to be apprehended, victims would equally be unable to obtain justice for whatsoever type of cybercrime they suffered.

[79] https://www.ibm.com, (accessed on the 14th of April 2025)

[80] Artificial intelligence tools have made phishing attack which is one of the most successful cybercrimes on financial institutions more sophisticated and accomplishable. For instance, cybercriminals can use “deep fake” tactics to enable them duplicate a voice and leave a voicemail.

Artificial Intelligence technologies are being leveraged to circumvent identity and authentication-based financial institution network defences and perpetrate other frauds. Financial crime perpetrators are increasingly using AI to create fake or altered documentation, audio files, and video recordings, leading to increasing fraud cases.[81]

5.2. Measures in Combating Cybercrimes

The prevailing nature of cybercrimes poses a number of challenges for banks, customers and state governments. These challenges faced in combating cybercrimes require more effective measures in order to mitigate the risks of cybercrimes. Some of these proposed measures to respond to cyber-ills are examined below.

5.2.1. Use of Secured Networks

Most Information Technology (IT) devices operate with the aid of networks. Networking is an essential part of communication methods. A Computer Network is the interconnection of several devices to exchange data and information. Networking is very essential in every businesses dealing with technology. It is a significant part of communication method and helps in the interconnection of several devices for the exchange of data and information.[82] Therefore, maintaining network security is essential for the safety of banks and their customers. The vulnerabilities that are found within the IT can easily be exploited by cybercriminals via internet networks. A virtuous network security system within the e-banking sector reduces the worry of data theft and interruption.[83]

5.2.2. The use of "Two-Factor Authentication (2FA)" Apps

Unauthorised access to confidential information is one of the biggest security threats to top banks and their customers. To mitigate this threat, banks and other organisations need to implement the multi-factor authentication. This will require further verification apart from having just the passwords. Banks whose financial services are highly dependent on IT should also implement the principle of least privilege, in which customers can only have access to data and systems necessary for their transactions. This will help to minimise the potential impact of compromised accounts.[84]

5.2.3. Establishing International Norms

Since cybercrimes involve a wider cyberspace, national laws should be corroborated with international norms relating to cybercrimes. States should not only rely on local laws they should corporate with other countries to form a secure and unified laws to combat cybercrimes.

[81] Sift, "Q2 2023 Digital Trust & Safety Index – Fighting Fraud in the Age of AI and Automation," June 22, 2023.
[82] Leukfelt Rutger & Holt Thomas J., (2020), *The Human Factor of Cybercrime*, First Edition, Routledge, London & New York, USA, P. 134.
[83] Network security helps in guarding terminals against dangerous spyware. It also certifies that shared data is kept protected. Network security has a co-relationship with cyber-security. Some of the ways in which network security ensures that the incoming and outgoing data traffic is safe are examined below.
[84] It is equally important to regularly review access rights since such review ensure the identification and revocation of access are no longer needed, which reduces cyber-attacks.

Though some international norms have been established by countries through conventions and treaties, they are very minimal and ineffective in responding to the dynamics and risks posed by cybercrimes.[85]

5.2.4. Abstention from Accessing Untrusted Sites and Emails

Banks and their customers are expected to adopt the zero trust security models. They should operate base on the principle that "never trust, always verify". This principle will help to effectively reduce unauthorised access and data infringements. This principle differs from other traditional security models, wherein the concept is based on the security at the perimeter. It is advisable that banks and their customers should always assume that they are available threats inside the network which require verification each time they want to access a link or emails. This help to build network segmentation, tight access and monitoring of users in relation to suspicious activities.

5.2.5. Keep Passwords Private

Passwords are backbones for the security of accounts irrespective of the type of account in question. Keeping passwords private is important for e-bankers and their customers in that, it helps to prevent unauthorised accessed to their credential information (sensitive information such as financial data).[86] Banks and their customers are not only advised to keep their passwords private, but they are also advised to establish strong passwords. Using strong passwords for accounts will make it difficult for cybercriminals or machines to guess their passwords. A good and strong password should have at least a minimum of 15 characters composed of letters (both upper and lower cases), and numbers, more especially for those who do not use the multifactor authentication.[87] Other security measures include; security training for banks' employees and customers, strengthen endpoint security, frequent change of passwords, the use of different passwords for different accounts/websites.

6. Conclusion

As technology is emerging, cybercrime keeps increasing and the challenges in combating such crimes are multiplying. The fight against cybercrimes is a continuous one and requires relentless efforts by both national and international actors not leaving out the role of each individual and private organization. The fast growing and changing nature of information and communication technologies is a threat to international order. The new crime-wave introduced by this technology which is known as 'cybercrime', poses a lot of challenges both at

[85] Many countries are reluctant in joining forces in the fight against cyber insecurity which is a global challenge to individuals, governments, organisations and businesses more particularly banks and their customers who are often the target of cybercriminals that are out for financial gain.

[86] According to the Verizon's Data Breach Investigation Report of 2020, over 30%of data breaches involved stolen credentials including passwords and usernames.

[87] Avoid the use of common passwords like the use of chronological numbers (1234), or the use of names as passwords. In order to create stronger passwords, banks and their customers can use a password manager that is capable of generating complex, long passwords. They should equally ensure that the password manager is from a legal and reputable company.

national and international level. Cybercrime is complex to tackle due to its dynamic and complex nature. The growing discrepancies of cybercrimes require an effective panacea that can respond to the challenges faced in combating cybercrimes. Establishing uniform international rules to regulate cyber offences will go a long way to ensure the prosecution of cybercrimes amongst states. This will also help to fill in the loopholes that are found in local legislations for cybercrimes.

Reference

1) Aazib Afraz T. & Geetha R., (2024), "E-banking: Opportunities and Challenges from Customer's Perspective", Vol. 4, *Qubahan Academic Journal*, Pp. 351-358.
2) Awah Harvey Ambe, (2022), "The Protection of Users of E-banking Services in Cameroon: A Legal Approach", Vol. 4, *Journal of Banking and Insurance Law*, Issue 2, Pp. 26- 37.
3) Batra Kumar N. & Gulat Parul, (2022), "Cyber-Attacks on Banking Institutions in India: Safety and Preventive Measures", vol. 2, *International Journal of Innovations & Research Analysis (IJIRA)*, Pp. 19-23.
4) Djieufack Roland and Awah Ambe Harvey, (2019), *Users of E-Banking within the CEMAC Zone: The Cameroonian Experience*. Éditions Universitaires Européennes.
5) Gercke Marko, (2009), *Understanding Cybercrime: A Guide for Developing Countries,* Geneva, International Telecommunication Union (ITU), Geneva, Switzerland.
6) https://63SATS.com (accessed on the 23rd of March 2025).
7) https://63SATS.com (accessed on the 23rd of March 2025).
8) https://www.63sats.com (accessed on the 25th April 2025).
9) https://www.63sats.com (accessed on the 5th April 2024).
10) https://www.hkma.gov.hk (accessed on the 10th of April 2025).
11) https://www.ibm.com, (accessed on the 14th of April 2024).
12) https://www.investopedia.com, (accesses on the 14th April 2025).
13) https://www.reviewtrackers.com/…/bank-reputation-risk, (accessed on the 16th of April 2025).
14) https://www.sentinelone.com , (accessed on the 12th of April 2025).
15) https://www.weforum.org (accessed on the 30th of March 2025).
16) https://yacenter.org>internet-banking visited on the 28th of April 2025.
17) Jurjen Jansen & Rutger Leukfeldt, (2016), Phishing and Malware Attacks on Online Banking Customers in Netherlands: A Qualitative Analysis of Factors Leading to Victimization" Vol. 10, *International Journal of Cyber Criminology*, Pp. 79-91.
18) Kaira Milani F., (2023) "Banking Malware Attacks and Security Solutions Review", Vol. 1, *Jurnal Penelitian Sistem Informasi (JPSI)*, Pp. 49-64.
19) Kumudha S. & Aswathy R., (2018), "A Critical Analysis of Cyber Phishing and its Impact on Banking Sector", Vol. 119, *International Journal of Pure and Applied Mathematics,* Pp. 1557-1570.
20) Leukfelt Rutger & Holt Thomas J., (2020), *The Human Factor of Cybercrime*, First Edition, Routledge, London & New York, USA.
21) LINEARSTACK (2023), "Preventing Data Diddling and Samali Attacks", available on www.linearstack.com (accessed on the 13th August 2024).
22) Okpa Martins M., (2022), "An Assessment of Cyber Crime in Commercial Banks in Calabar Metropolis, Vol. 11, *Ibom Journal of Social Issues,* Pp. 20-35.
23) Ranny Caroline & Miniawati Tina V. B., (2025), "Analysis of Pharming in Cyber Crime and its Impact on Customer Trust (Case Study on Bank BRI Customer Bandar Lampung Regional Office)", Vol. 3, *International journal of Accounting, Management, Economics and Social Sciences,* Pp. 259-270.

24) Shea John M., (2013), *Combating Computer Viruses*, 1st Edition, Gareth Stevens, New York, USA.
25) The Law on Cybersecurity and Cybercriminality in Cameroon.
26) The Law on Electronic Commence in Cameroon.
27) The Law on Personal Data Protection in Cameroon.
28) Vidhya Jolly, (2016), "The Influence of Internet Banking and cost Savings for Banks' Customers", Vol. 3, Nepal, *International Journal of Social Sciences and Management,* issue 3, Pp. 163-170.
29) Vijay Ramalingam, (2019), "Impact of Hacking on Cyber Security", Vol. 6, *Journal of Emerging Technologies and Innovative Research*, Pp. 132-136.
30) Viraja V.K. & Pradnya Purandare, (2020), "A Qualitative Research on the Impact and Challenges of Cybercrimes", *Journal of Physics: Conference Series,* Pp. 1-11.
31) Wangui Phelista N., (2019), "Investigating extent to which Cybercrime Influences Performance of Commercial Banks in Kenya", United Kingdom, Vol. VII, *International Journal of Economics, Commerce and Management*, Pp. 489-514.
32) Yuniawati Y. et al., (2021), "Factors Detecting Employee Fraud: A Study Among Private Companies in Jarkarta", Vol. 570, *Proceedings of the International Conference on Economics, Business, Social and Humanities*, Pp. 503-510.