JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

ONLINE BANKING FRAUD RISK AND AWARENESS

Submitted By

STUDENT'SNAME	REGISTRATION NUMBER
Pankaj Sahani	**12202204**
Srishti Sharma	**12223292**
Guruvinder Singh	**12202414**
Bharat Sharma	**12210603**

In partial fulfilment of the requirements for the award of the degree of

MASTER OF BUSINESS ADMINISTRATION (MBA)

LOVELY PROFESSIONAL UNIVERSITY

Supervisor: Dr. Nitin Gupta

Chapter 1:

Introduction:

In a technology ruled with the aid of digital transformation, online banking has emerged as a cornerstoneof modern-day financial offerings, offering remarkable ease and accessibility to customers globally. However, along with the proliferation of on-line banking offerings, the chance of internet banking fraud has emerged as a big subject. Malicious actors, leveraging sophisticated strategies inclusive of scams, malware assaults, and social engineering techniques, pose a powerful risk to the safety of virtual monetary transactions. As a result, both purchasers and economic institutions face mounting demanding situations in safeguarding sensitive financial information and mitigating the dangers associated with on-line banking fraud.

Online banking, which provides customers with unmatched ease and accessibility worldwide, has become.

A key component of financial services in the age of digital transformation. But the widespread risk of online banking fraud is a growing worry that has been brought on by this technical innovation. The picture of risk is changing as more financial transactions are conducted on digital platforms, posing new difficulties for both consumers and financial institutions.

The expertise of hackers, who persistently take advantage of weaknesses in the digital financial environment, highlights the widespread nature of online banking fraud. Malicious actors attempting to get unauthorized access to confidential financial data are increasingly using tactics like scams, malwareattacks, and social engineering. If these attacks are successful, people and organizations may suffer significant financial losses, identity theft, and unlawful transactions.

This examines objectives to offer a complete review of studies performed on internet banking fraud, hazard recognition, and associated elements. by inspecting numerous dimensions of the hazard panorama, including the influence of risk variables on users' intentions to retain using net banking, security features for detecting and stopping e-banking fraud, customer perceptions of chance, and factors affecting the adoption of net banking, this study seeks to elucidate the multifaceted nature of the demanding situations posed with the aid of on-line banking fraud.

Key findings from current studies underscore the importance of perceived usefulness, social danger, time loss risk, possibility value threat, and mind-set in the direction of continued utilization as pivotal determinants of customers' intention to persist with internet banking. Moreover, the studies emphasize the important need for more desirable security measures, which includes the identity of malware producers, evaluation of safety strategies and frameworks, and implementation of sturdy fraud prevention structures. Additionally, the studies highlight the significance of patron education and attention programs in organizing trust in on-line banking and safeguarding personal information.

Furthermore, this takes a look at acknowledges the demanding situations confronted via law enforcement companies and regulators in fighting cybercrime. To deal with those demanding situations, the research proposes leveraging semantic technologies, information mining strategies, and facts analysis to strengthen cybercrime investigations and enhance fraud detection abilities. through fostering

collaboration between banks, regulators, policymakers, and era specialists, this studies objectives to increase effective strategies for mitigating the dangers related to internet banking fraud and promoting awareness amongst stakeholders.

Typically, this study underscores the continued need for research and improvement in addressing net banking fraud risks and improving security features. by means of presenting valuable insights to banks, regulators, and policymakers, this research ambitions to empower stakeholders to take proactive steps in combating cyber threats and safeguarding the integrity of digital financial transactions.

E-banking risks: Operational and security dangers

Operational danger: Operational hazard, additionally called transactional threat, is one of the most common sorts of e-banking hazard. It encompasses various capacity troubles, including processing transactions incorrectly, recording privacy and confidentiality compromises, unauthorized get right of entry to to the bank's structures, and different operational inefficiencies. As online banking transactions become increasingly more complicated and interconnected, the risk of operational failures and mistakes escalates, posing full-size demanding situations to financial institutions and their clients.

safety hazard: the safety of on-line transactions is paramount while discussing e-banking dangers. whilstpurchasers assume the privateness and security of their transactions, the pervasive nature of online banking exposes them to numerous protection threats, which include hacking, unauthorized entry to bank systems, and facts breaches. As cybercriminals hire an increasing number of state-of-the-art strategies to exploit vulnerabilities in online banking structures, economic establishments must continually enhance their safety features to defend consumer information and save you from fraud.

according to the Deloitte India Banking Fraud Survey, version-IV, there is a substantial notion most ofthe public that banking frauds will boom within the coming years. elements contributing to this notion include the huge-scale faraway-running model, the developing adoption of non-department banking channels which include on-line net banking, and the inefficiency of forensic gear in figuring out capability purple flags of banking measurements. The survey highlights diverse fraud schemes accepted in banks, including data robbery and cybersecurity breaches, underscoring the urgent want for strong fraud prevention measures.

The developing chance of online Banking Fraud

With the increasing adoption of net banking, the danger of fraud is rising daily. As human beings lead more gadget-orientated lives and feature much less time to go to financial institution branches, online banking offers unparalleled convenience and accessibility. but this convenience comes with inherent risks, as cybercriminals take advantage of vulnerabilities in on-line banking systems to perpetrate fraud.approximately 65% of all fraud cases stated through banks are era-related, protecting frauds devoted through ATMs, net banking channels, and different fee channels including credit, debit, and prepaid cards.

To combat the developing danger of on-line banking fraud, it’s vital to study the diverse dangers relatedto online banking comprehensively. Those dangers include negligent financial institution control, fraudusing QR codes, and attacks regarding phishing, smishing, or vishing. By way of elevating attention of these problems and enforcing powerful fraud prevention measures, financial institutions can mitigate the dangers posed through online banking fraud and protect their clients' monetary belongings.

The significance of research and attention

This venture's aim is to recognize how online banking frauds occur, improve public focus of them, and verify their effect. The look at specializes in numerous key goals, including identifying vulnerabilities in on-line banking structures to reduce the hazard of fraud, informing consumers approximately traditional strategies used by internet banking scammers to raise consciousness, evaluating the effectiveness of regulatory frameworks in combating net banking fraud, and growing progressive technologies and strategies to beautify detection and prevention of online banking fraud.

Overall, being aware of the risks associated with online banking and taking steps to protect yourself canhelp ensure that your personal and financial information stays safe.

E-banking risks. Here are some specific e-banking risks:

Operational Risk: The most typical kind of e-banking risk is operation risk, often known as transactional risk. As it contains: processing transactions incorrectly, Data privacy, confidentiality, and data integrity compromises, Access to the bank's systems without authorization, etc.

Security Risk: The security of the transaction is of the utmost importance when discussing bank transactions. Every consumer wants the privacy of their transactions. However, everything is availableonline, there is always a danger that someone could get the data and use it inappropriately. Threats of hacking and unauthorized access to the bank's systems are additional sources of e-banking security risk.

Scope:

Focus on specific user behaviors:

1. Examine the connection between users' intentions to keep using online banking and perceived risk considerations (such as security, privacy, and social risk). To learn about the concerns and motives ofusers, surveys and interviews may be conducted.

2. Examine user behavior data to find trends that point to fraudulent activities. This can entail identifying questionable transactions or login attempts using machine learning techniques. Assess how well various educational initiatives have worked to increase consumer awareness of online banking fraud. This could entail evaluating various educational resources and calculating how theyaffect users' behavior and knowledge.

Focus on specific types of fraud:

1. Examine the precise techniques, such as phishing, malware, and social engineering, that scammers employ to target consumers of online banking. This could entail performing penetration testing to find vulnerabilities or evaluating already- published fraud reports.

2. Examine how technology can either help or hinder online banking fraud. This can entail assessingthe efficacy of various security precautions, such encryption or two-factor authentication.

3. Examine and evaluate the legal and regulatory structures put in place to stop online banking fraud. This can entail contrasting the methods used by various nations for regulation and enforcement.

Focus on broader societal implications:

1. Examine the financial and societal repercussions of internet banking fraud for financial organizations as well as for people. This can entail calculating the monetary damages brought on byfraud as well as the effect on public confidence in the financial system.

2. Examine the financial and societal repercussions of internet banking fraud for financial organizations as well as for people. This can entail calculating the monetary damages brought on by fraud as well as the effect on public confidence in the financial system. Examine the security of online banking going forward and note any new developments or difficulties. This could entail investigating novel fraud-prevention technology as well as the possible effects of regulatory landscape modifications.

The ideal scope for your project will ultimately rely on your unique interests and level of experiencein addition to the resources at your disposal. Nevertheless, I hope that these recommendations have provided you with a foundation for refining your focus and formulating an impactful and pertinent research question.

It's crucial to remember that the material supplied is restricted to the abstract and introduction; in orderto decide on the ideal scope, a more thorough comprehension of the research topic would be required.

Need of the study:

The risk of fraud is rising daily along with the use of internet banking. People today are more educatedthan in the past, therefore their lives are more machine-oriented and they have less timethan ever beforeto visit a bank branch. When a consumer has access to an internet-connected computer, they can do theirbusiness without having to go to a bank branch. Simply put, if they have an internet connection, they can transact anytime, anyplace. Customers can obtain a range ofservices, such as a request for a checkbook or a balance query, by dialing the telebanking number.While a significant portion of fraud cases were advance-related, approximately 65% of all fraud cases reported by banks were technology- related frauds (covering frauds committed through ATMs, internet banking channels, and other paymentchannels like credit, debit, and prepaid cards).

Due to these factors, it is imperative that one studies the risks associated with online banking. These include negligent bank management, fraud using a QR code, The main causes are attacks involving phishing, smishing, or vishing. One must be aware of these issues and act as soon as possible to combatfraud and awareness. To do this, one must conduct training programmes for fraud awareness improvements in policies. Without the survey, it would be impossible to identifythe full scope of the online banking fad, which is why it is important. Finding the cause of varioustypes of fraud allows one to take action to manage or prevent them. Consequently, it is vital to thoroughly research Online BankingFraud Risk and Awareness.

Chapter 2:

Literature review:

Pankaj Kumar Gupta (2008): Since the late 1990s, as electronic commerce has grown, therehas beena rise in interest in Internet banking in emerging nations. Studies have demonstrated that Internet banking can result in cost reductions, revenue growth, and higher customer happiness, making it a desirable tool for creating a sound strategy. Government and finance
authorities are now faced with difficult public policy decisions due to the paucity of systematic. information about Internet banking in India. This paper fills in these knowledge gaps by looking at consumer perceptions of Internet banking, its growth currently, and prospective developmentsin the future. The weaknesses of conventional banking are emphasized, client knowledge of online banking isinvestigated, and prospective effects on bank strategy are described. Aspects of regulation and supervision pertaining to online banking are also covered.

Marinela Vrincianu and Liana Anica Popa (2010): Each year, there are several reports of security flaws in the electronic banking (e-Banking) system, highlighting the need for clients to be protected and made aware of the possibility of being subjected to harmful activity carried out by cybercriminals. Consumers and financial institutions are aware that more sophisticated criminals are carrying out increasingly sophisticated attacks and financial scams. Technology is akey component of this class's strategy as they get more advanced. The experts also predict that.
The present global recession would probably lead to an increase in internal fraud and security breaches. Through a thorough review of the pertinent literature, the current study attempts to: (1)analyze the potential threats posing a security risk to e-banking services; (2) identify the tools and techniques that can guarantee the protection of customers in e-banking, (3) to share the findings of a pilot study on Romanian consumers' perceptions of E-Banking services' protectionand security.

Wadie Nasri (2011): This essay's goal is to identify the variables that affect Tunisia's adoption ofonline banking services. The adoption of internet banking is conceptualized and linked to variouselements using a theoretical model that is presented. A total of 253 Tunisian respondents were sampled for the following questions: 95 involved online banks. 158 people did not utilize an
internet bank. Regression analysis and factor analyses are used to investigate the link. The
model's findings made it abundantly evident that convenience, risk, security, and prior internet expertise are the factors that have the most impact on Tunisia's use of online banking. Only knowingabout online banking did not change Tunisia's determination to adopt the service.
Additionally, the findings suggest that demographic characteristics have a considerable impacton internet banking habits, particularly instruction. This study concludes by arguing that.
practitioners who plan and promote new forms of banking in the current competitive market. must have a thorough awareness of the variables influencing intention to utilize internet banking.

According to Prof. Rachel Barker (2011): The knowledge management paradigm shows howthe gathering,

sharing, and assimilation of information can be used to manage and control.
messages in an online crisis and communication response scenario by maximizing consumers' motivation and capacity to act in response to perceived online-transaction risks. In order to secure output control and the security of online banking transactions, it thus proposes an approach that relieson people's motivation and empowerment. The purpose of this article is topresent a comparative examination of knowledge management of online crisis-communicationresponses in relation to fraudulent financial transactions in one of South Africa's top 10 banks during two particular time periods.

According to Prof. Rachel Barker (2011): This article discusses the impact of globalization and technology on the banking business, which has resulted in the need for financial institutions to adapt tothe internet market and overcome consumer concerns about fraudulent online
transactions. While there has been research on the adoption of self-service technologies, littleattentionhas been paid to managing online crisis-communication responses in the context of online security. Inorder to control and regulate messages, the study advises adopting the knowledge management technique to efficiently collect, transfer, and absorb information in online crisis communication response settings. Over two years, a comparative study of the knowledge management of online crisis-communication responses in relation to fraudulent financial transactions at one of South Africa's top 10 banks will be conducted.

According to Article by Ahmed Kabir Usman, Mahmood Hussain Shah (2011): According
to this article, electronic banking fraud is globally and is expensive to both banks and consumers. Electronic banking frauds occur as a result of the Weak Authentication System and Internal Control Systems, this area has not been researched as well as there has been no proper research on how to improve online security and prevent shareholders to lose the trust in the upcoming
technology related to online securities. The purpose of this research was to bridge the gap.
between success of online security and strength of fraud preventions in electronic banking, by determining that above technology, there are several other factors which affect the Online Banking Security, which can be internal, external or dependent upon Education which willregulate the information specific areas needed to be made on Fraud Prevention Systems.

Wei Wei, Jinjiu Li, Longbing Cao, Yuming Ou & Jiahang Chen (2012): This study presents asystem for identifying online banking fraud by merging multiple data mining algorithms and profiling the distinguishing rate of each transaction based on the client's behaviour preference.
The system use the Difference Mine algorithm to mine contrast patterns and distinguish between fraudulent and authentic behavior, followed by an effective pattern selection and risk assessmentthat integrates predictions from several models. The system was evaluated on large-scale real- world online banking data and achieved much improved accuracy and reduced alert volume when compared to benchmarking fraud detection systems employing domain knowledge and
traditional fraud detection methodologies.

According to Arvid O. I. Hoffmann and Cornelia Birnbrich (2012): This study aims to establish aconceptual and empirical correlation between retail banks' efforts to safeguard their clients from third-party fraud, the caliber of client interactions, and client loyalty. A conceptual framework is created connecting customer familiarity with and knowledge of fraud protection methods, good customer relationships, and customer loyalty. Data was obtained in conjunction.
with a major German retail bank in order to empirically test the conceptual framework. Customer familiarity and awareness of fraud protection techniques were found to be positively correlated with customer relationship quality

as indicated by satisfaction, trust, and commitment. As
determined by intents to maintain their relationship with and purchase additional goods fromtheirbank, the quality of customer interactions is also positively correlated with customer.
loyalty. The findings highlight the significance of fraud prevention for retail banks and
demonstrate that, in addition to the financial goal of lowering operational costs, fraud preventionand itssuccessful communication are an important means of enhancing the quality of client
relationships and, ultimately, customer loyalty.

Ankit Kesharwan & Trilochan Tripathy (2012): This article looks at how perceived risk has influenced internet banking uptake over the last two decades, focusing on both internal and
external influences. As part of the study, a questionnaire was issued to 362 non-Internet banking users, and a multiple regression approach was utilized to investigate the impact of various risk variables on Internet banking uptake. According to the findings, privacy, security, social, and performance concerns, as well as computer self-efficacy, all have a significant impact on Internetbanking uptake. The study underlines the importance of assessing perceived risk as a critical component of Internet banking adoption.

Nicole S. van der Meulen (2013): In instances of Internet banking fraud, how consumer culpability ishandled is critically explored in this article. Although banks typicallyreimburse each victim of Internet banking fraud for their financial losses, there are occasionallyexceptions, at least in several EU memberstates. They do, however, point to a variety of (legal)issues but are hardly ever discussed. Concerning whether a customer might be held accountable, the primary issue is a lack of transparency and consistency. These issues also preserve the possibility of unfavorable outcomes, such as a rise in perceived danger, a breakdown in trust, andrequests for better security, all of which may not be the mostadvantageous from an economic standpoint. The potential advantages of introducing zero liability as analternative are discussed.

Shah, Mahmood (2013): E-banking fraud is an issue that is faced on a global scale and that continues to cost money for both banks and customers. Fraud in e-banking services is carried onby a variety of security flaws, from inadequate internal controls to poor verification systems.
Since there is a dearth of research in this area, it is problematic for practitioners; therefore, research needs to be done to help improve security and keep stakeholders' faith in the system.
The goal of this essay is to better understand the variables that might be important for enhancing electronic banking fraud prevention systems. The purpose of this study is to identify potential key success factors for the prevention of fraud in e-banking systems by reviewing relevant research. Our research shows that in addition to technology, there are other factors that must be
Take into consideration, including internal controls, customer education, training for employees,etc. These findings will provide banks and regulators with information on areas that should be addressed to improve their current fraud prevention efforts.

Rashidah Abdul Rahman a, Irda Syahira Khair Anwar (2014): This study seeks to shed lighton how bankers see the efficiency of fraud detection and prevention measures in Malaysian Islamic institutions. The results of 146 questionnaires given to managers and officials of Islamic banks in Malaysia showed that the most successful elements of fraud prevention measures were the protection software/application. In contrast, when evaluated separately, bank reconciliation, password protection,and internal control review and improvement stand out as the most successful strategies. In terms of assessing Malaysia's present degree of bank fraud prevention,
this study should be useful to both academics and practitioners.

According to Dr. N. J. Uke, Samir Pakojwar (2014): The utilization of online service access isgrowing inthe modern world. Internet banking is one aspect of this that is quickly expanding.
The banks shall use "best of breed" technologies to authenticate customers' identities when theylog inand to ensure that their data is delivered securely and consistently in order to provide
clients with a safe, reliable, and consistent online environment in which to conduct online banking. The bank should develop the best backup and emergency plans as well as the best security practices. This essay aims to examine a variety of technologies and security standardsthat various researchers have suggested to banks for secure internet banking and to compare anumber of security programs based on the suggestions made by these authors.

Carolina Martins, Tiago Oliveira, Aleš Popovic (2014): Banks and users alike should be awareof the crucial factors influencing the adoption of Internet banking as a result of this study, as we presently know little about how consumers' perceptions of risk affect this adoption. In response, we create a conceptual model to capture the behavioral intent and usage behaviors of Internet banking by fusing the unified theory of acceptance and use of technological devices (UTAUT) with perceived risk. The conceptual model was put to the test using data from Portugal (249 validexamples). Our results also provide evidence for other UTAUT linkages and support the roles of risk and effort as better predictors of intention than performance expectancy, effort expectancy,and social influence.

According to a study by Shewangu Dzomira (2014): Through the analysis of questionnaire
material and interviews with informants from 22 banks, the study looked into electronic fraud in the banking industry. According to the survey, the banking sector was the target of the majority of electronicfraud schemes. Other problems included inadequate cybercrime laws, inadequate resources, a lack of information and awareness, and ineffective legislation. In order to lower risk,the report recommends involving all interested parties in the discussion of cybersecurity to safeguard technological infrastructure from online attacks.

Rodrigo Carvalho (2015): This paper highlights the difficulties faced by law enforcement authoritiesin countering cybercrime due to the vast number of data to be analysed and the limitsof standard investigation approaches. The paper recommends using semantic technologies, notably an ontology, to improve the efficiency of cybercrime investigations. The ontology seeksto map criminal companies and detect malware makers, with a focus on online banking fraud.
The study recommends extending current ontologies and creating new abstracts to improve relationship discovery, as well as adopting empiricism-based inference procedures to bettersatisfythe needs of human analysts.

Normalini Md Kassim And T. Ramayah (2015): This paper highlights the difficulties that law enforcement organizations have in countering cybercrime because of the vast number of data thatmustbe analysed and the limits of traditional investigation approaches. The study suggests that semantic technologies, notably ontologies, be used to increase the efficiency of cybercrime
investigations. With an emphasis on online financial fraud, the ontology tries to map criminal companies and detect malware makers. To improve relationship discovery, the study recommends extending existing ontologies and creating new abstractions, as well as adoptingempiricism-based inference rules to better satisfy the needs of human analysts..

Rute Abreu, Fatima David, Mena Legcevic, Liliane Segura, Henrique Formigoni, Flavio Mantovani (2015): This study contends that ethics should be utilized to address security risksand weaknesses in electronic financial systems. It underlines the importance of being a good citizen by refraining from damaging activity and

encouraging accountability and social responsibility. The research examines publicly available data from the Portuguese Banking
Association and depends on studies on ethics, fraud, and ICT in e-banking services. The findings emphasize several risks and flaws connected with e-banking services, as well as the necessity of public debate in creating ethical guidelines and decreasing fraud. Finally, the essay emphasizes
the importance of encouraging responsible behavior and transparency in order to reduce risksand assure the continued availability of e-banking services.

Madan Lal Bhasin (2015): Bank fraud is on the rise in India, posing a serious threat to the financial sector's growth. Poor employment practises, ineffective staff training, weak internal control systems, and low compliance rates were identified as factors contributing to the problemin a survey of 345 bank workers done in 2012-2013. However, proactive actions such as
conducting risk studies of processes and laws may lower the risk of possible fraud-related losses.
Technology can also help in the battle against fraud by utilizing forensic information analysis and data mining tactics. To combat contemporary scams, it is critical to focus on enhancing banksecurity features.

Khulood Al Zaabi Abdallah Tubaishat (2015): Due to the increased demand for electronic payments and a resulting increase in fraud strategies, the banking sector globally suffers annual
losses of millions of dollars. Much research has been conducted to identify solutions for securinginternetpayments and preventing fraud in the banking sector. But none of these studies has produced a thorough client banking education program. As a result of this study, the Information Security Awareness program, or ISAP, is a suggested awareness program. We believe that this kind of program is necessary for the following reasons: To promote customer trust in online banking, protect each client's personal information, and follow the guidelines set forth by online banks. In the following areas: online purchasing, online protection, password protection,
operating system protection, identity theft protection, and debit/credit card protection, we have identified several online scams and then proposed some best practices for online protection.

Jaafar M. Alghazo, Zafar Kazmi, Ghazanfar Latif (2017): This paper investigates the securityof internet banking in three developing countries and recommends a plan to lessen the risk of cyber securitybreaches. The study is based on surveys performed in Saudi Arabia, Pakistan, and India, which focusedon customers' online banking habits and their understanding of cyber security issues. The findings indicate a growing gap between user behaviors and bank
expectations, which the proposed strategy attempts to solve by giving banks more responsibilityfor reducing user cyber security risks. Overall, the paper highlights the need to tackle cyber security concerns in internet banking to ensure safe and secure transactions.

Shewangu Dzomira (2017): This study investigated how electronic banking services and plasticmoney are promoted in connection to financial identity theft fraud risk awareness in Zimbabwe'sbanking sector via bank websites. Data from 14 randomly selected bank websites were studied using qualitative content analysis research methodology. The findings show that, while the general public in Zimbabwe is increasingly accepting plastic money and computerized banking, bank consumers have limited understanding of financial identity theft. According to the paper, banking institutions should immediately focus on and benefit from the use of plastic cards and
electronic banking, while simultaneously increasing awareness among users of these services about themany types of financial identity theft fraud. Financial identity theft information should be widely available and shared with

clients.

According to Prof. Rachel Barker (2018): The growth of e-banking has resulted in an increase in fraudulent activity, prompting financial institutions to advise users to discern between fraudulent and genuine transactions. However, there is still a lack of clarity on when customers have acted irresponsibly, resulting in a loss of trust and the need for greater security. To solve thisissue, this research examines knowledge management critically and presents an approach for e- banking fraud prevention and co-liability through proactive interaction. The framework has fraudprevention measures, e-securitymeasures, and legal consequences in order to limit negative.

outcomes for both the banking sector and clients. The purpose is to increase customer trust and security in e-banking.

According to Article by Paul van Schaik, Jurjen Jansen (2018): It gives an insight on what isthe behavior of Customer/User related to Online Banking and how it can be an important tool totackle the problem of Online Banking fraud. In this article, a questionnaire session was done for1200 people whoperform online banking in their day-to-day life in the European country of
Netherlands. While on several parameters, the results were generated partial-least-squares path- modelling method which made several hypotheses, which showed high levels of variance for risk perceptions and precautionary consumer behavior, the two of the most important factors are: ResponseEfficacy and Self- Efficacy.

Oluwalami Matthew Fadayo (2018): Using mixed research approaches, this study analyses theissuesof e-banking fraud prevention and detection encountered by Nigerian financial
institutions. The study identifies several contributing factors to the rise in e-banking fraud inNigeria, including inefficient banking operations, internal control issues, a lack of customer awareness and staff training, inadequate infrastructure, sophisticated technological tools available to fraudsters, and bank staff negligence. The study proposes a new paradigm for e- banking fraud prevention and detection, emphasising the importance of technological
mechanisms, fraud monitoring, effective internal controls, consumer complaints, whistleblowing, surveillance, institutional synergy, staff-customer awareness and education, as well as legislativeand judicial oversight. The findings have significant implications for policymakers, financial
institutions, anti-fraud organization researchers, academics, and accounting professionals in boththe public and private sectors. Implementing the recommended

Rachel BARKER (2018): The rise of e-banking has resulted in an increase in cybercrime,
including identity theft, phishing, vishing, smishing, and malware use. Proactive communicationand knowledge management can assist boost customer awareness and improve client
relationships. This study employed a qualitative approach to investigate the South African Banking Risk Information Centre's (SABRIC) website research strategy and discovered that proactive consumer education is critical in preventing victimization. Transparency in security practises and standards can also encourage shared accountability and liability rules. Overall, thestudy emphasizes the significance of teaching clients about e-banking fraud protection
techniques and creating a teamwork approach when it comes to security.

Mostafa A. Ali, Nazimah Hussin Ibtihal A. Abed (2019): suggested that Customers are happywith e-banking because they get better service, and banks profit from its competitive edge.
However, even today, many customers are still put off from utilizing the service by the
inadequate e-banking security. This is a result of fraudsters' deceitful behaviors. In this work, thesecurity concerns

associated with e-banking have been explored and resolved. The challenges and characteristicsof e-banking fraud have also been imitated. This essay also covered numerousmethods for detecting attacks and fraud as well as certain security measures for e-banking services. In this research, different e-banking security techniques and frameworks were evaluatedaccording to expert opinion.

Ivan Skula, Jan Bohacik, Michal Zabovsky (2020): As a consumer of a bank, insurance firm, mobile operator, government agency, and many other businesses, each person runs the danger of becoming a victim of fraud. It is not enough to integrate fraud-risk-related procedures into routine business operations and to deploy fraud detection and prevention tools and systems. The employee or consumer, especially the less educated one, is typically the weakest link. As a result,it's crucial to combine the aforementioned actions with awareness and education. In this study, we examined the various fraud prevention awareness campaign channels and the factors (reach, relative cost, age group, and supportedmessage format) that affect their applicability.
Additionally, previous instances of messages relating to fraud as well as fraud were examined.
Banks in the UAE delivered informational updates on Twitter, one of the "youngest" social
media platforms. We looked at the tweets of a few selected banks in the United Arab Emirates tosee how they interact with their clients and, more especially, how they spread the word about fraud.

Iftikhar Ahmad, Shahid Iqbal, Shahzad Jamil, and Muhammad Kamran (2021): Digital scams have experienced a revolution because of the digitization of the banking sector. E-bankingscams are currently a problem on a global scale and have developed into an appealing business for hackers, whouse cutting-edge equipment. the use of malware, phishing, trojans, viruses, denial-of-service attacks, and identity theft tools. This study conducted a thorough assessment ofthe literature, identifying the technologies now used by banking institutions to secure the e- banking system as well as the methods responsible for its security flaws. Online databases such Emerald Insight, Google Scholar, IEEE,
JSTOR, Springer, and Science Direct were used for the
study's article sources. The in-depth examination provided a glimpse of the situation as it is todayand highlighted unique security measures that can successfully offset adverse consequences.

Pallavi Sood and Puneet Bhushan (2022): The banking industry in India has rapidly grown since the economy was liberalized in 1990–1991; however, there are currently significant problems with bank fraud. The Reserve Bank of India is in charge of overseeing the banking sector's regulation, but becausethe sector doubles as a target for fraud and a regulator, it presentsa dilemma to the government. The study examines bank fraud incidents that were reported to the Commission of Central Inspection, looking at underlying factors, financial instruments used, andregulatory flaws. Using secondary data and an interview-based technique, the investigation of allparties involved in reporting, regulating, and dealing with financial fraud was carried out. The study suggests that actions be made now to prevent fraud in the Indian banking industry in the future

Chapter 3:

Research methodology:

Questionnaire:

1. Have you ever used internet banking?
2. How frequently do you use internet banking?
3. Have you ever experienced any fraudulent activity while using internet banking?
4. Are you aware of the risks associated with internet banking?
5. Have you taken any measures to protect yourself from internet banking fraud?
6. What are the key determinants of your intention to continue using internet banking?
7. Do you think enhanced security measures are necessary to prevent internet banking fraud?
8. Do you think customer education and awareness programs are effective in establishing trust in online banking?
9. What steps do you think banks, regulators, and policymakers should take to mitigate the risksassociated with internet banking fraud?
10. What are the suggested program areas for customer education and awareness programs?

Gap Analysis:

Despite the bulk of the reviewed research stating as much, there is a lack of empirical evidenceto support the claims that Online Banking offers client's greater convenience and banks a
reduction in workload. The bulk of studies used a qualitative, expert opinion-based, or customersurvey technique, which provides a limited understanding of how Online Banking has an impacton both the public and the Banks. Future research should employ a quantitative
methodology to provide more compelling evidence of the influence of Online Banking Direct onthe performance of banks and the expansion of online banking in India.

The studies under consideration indicate that India's adoption of online banking is difficult. Littleis known, however, about the specific issues that banks and the public occasionally face. Future studies should identify the risks and challenges associated with using online banking in India and suggest solutions.

Most of the study under consideration focuses on the impact of fraud on both the general population

and banks, ignoring the variances among the fraudulent actions. In order to provide more targeted recommendations, future research might look at how the government and bankingregulatory bodies take severe action against those who are involved in fraud.

The impact of online banking on bank success and public convenience: More research is neededto understand how online banking affects banks and the people utilizing it, even though it is
important today due to its many benefits and risks. Future studies could examine global awareness to have a greater favorable influence.

For clients and banks to be aware of the hazards associated with online banking fraud in advance, more study is required to set policies for online payment app developers and theprograms they introduce.

There is still one unfilled research gap. Much useful research is being conducted in the area of onlinebanking fraud risk awareness. to inform the consumer. How effective these tactics are inactual use isunknown.

There is currently a significant lag in this study of how these thefts affect the company and thebank. It is vital to learn how to recover client trust following a fraud incidence and avoid long-term damageto their reputation online.

Objective of study:

This project's goal is to understand how online banking frauds occur, how the government raises.public awareness of them, and what impact they make. The study is focused on the following goals:

1. To reduce the risk of fraud, find vulnerabilities in online banking systems.
2. To raise awareness, inform consumers about typical strategies used by internet banking scammers.
3. Assessing how well regulatory frameworks perform to combat issues with internet banking fraud.
4. Develop innovative technologies and strategies to enhance detection and prevention of online banking fraud.
5. Evaluate the effectiveness of regulatory frameworks in combating internet banking fraud.

By focusing on these objectives, the study hopes to further the existing discussion on the safety of financial transactions conducted online and the teamwork required to safeguard the digital financial environment. It seeks to give banks, regulators, lawmakers, and technology specialists insightful information so they can beproactive in reducing the dangers of online banking fraud and raising customer awareness.

Research Design:

For the research we collected the primary data with the help of a questionnaire in primary data we made 10 questions related to our topic. We kept the sample size of 50 different types of individual questionnaire.

1. **Primary Research Method:** To collect quantitative data on participants' experiences, perceptions, and

behaviors linked to risk awareness and internet banking fraud, a structured questionnaire will be sent. Weuse the questionnaire for the collecting the information related to given below:

- To determine how often users use internet banking and how frequently users use online banking.
- To investigate participants' encounters with fraud when utilizing online banking.
- To gauge participants' knowledge of the dangers of online banking.
- To ascertain the precautions participants have made to guard against online banking fraud.
- To determine the main factors influencing participants' decision to keep using online banking.
- To find out what the participants think about how customer education to build internet banking confidence.
- To investigate suggestions made by participants for reducing the dangers of online banking fraud.

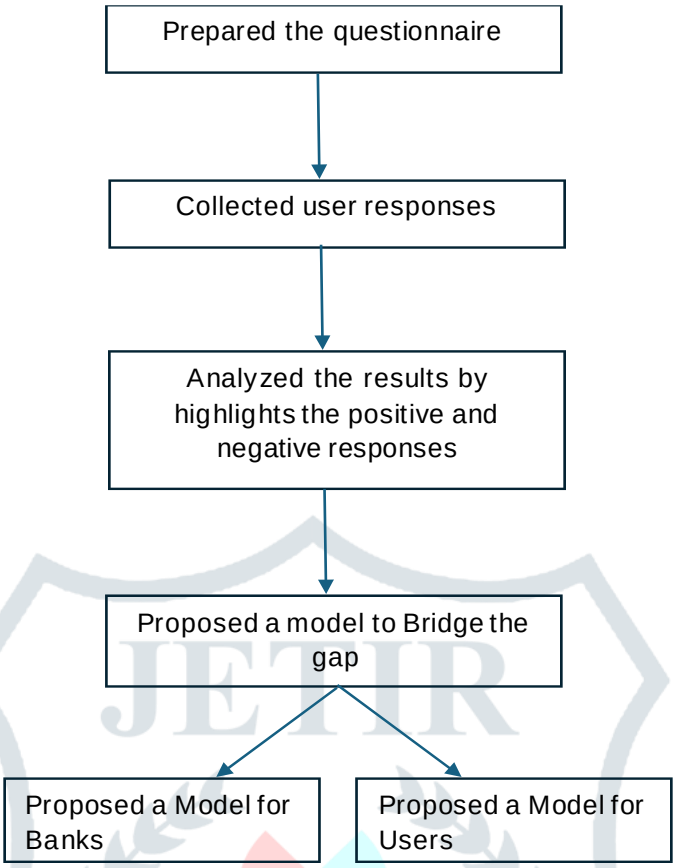
2. Sample Size: To provide a sufficiently large dataset to draw significant findings while simultaneously retaining manageability and feasibility, the study's sample size will be 50 participants.

3. Sample Method: Convenience sampling will be used to identify study participants, with an emphasis on people who are willing to participate and have prior experience with online banking. Multiple methods, including email lists, social media sites, and online forums, can be used for recruitment.

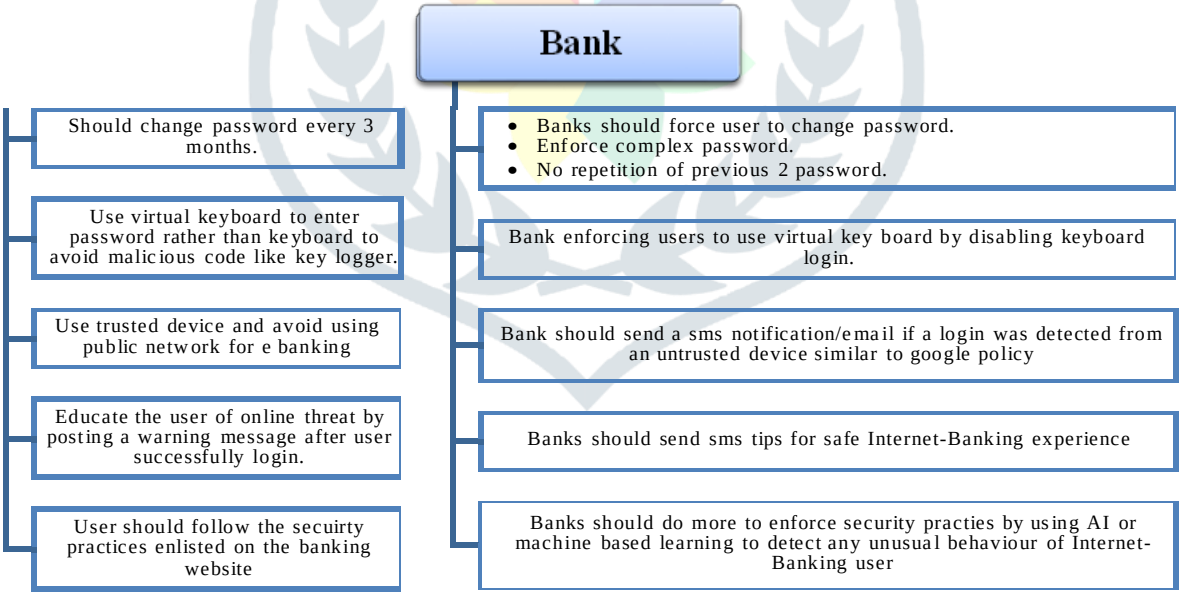
4. Instrument for Gathering Data: Every one of the 10 questions listed in the attached questionnaire will be covered by the one that is created. There will be closed-ended.

Here is the questionnaire with the responses for reference:

Bank



User



In order to reduce security risks in online banking, a proposed security model is prepared.

Chapter 4:

Empirical Analysis:

Questionnaire Analysis and Discussion:

1. **Have you ever used internet banking?**

Response: 93.2% of respondents have used internet banking.

Analysis: The overwhelming majority of respondents indicating they have used internet bankingsuggests a high level of adoption and reliance on online banking services.

Discussion: This high adoption rate highlights the importance of understanding user behaviors, concerns, and preferences to enhance the security and usability of internet banking platforms.

2. **How frequently do you use internet banking?**

Response: Daily (18.2%), Weekly (15.9%), Monthly (59.1%), Rarely (6.8%)

Analysis: The majority of respondents use internet banking on a monthly basis, followed by daily and weekly usage.

Discussion: Understanding the frequency of usage provides insights into the level of integration of internet banking into individuals' financial routines and the potential exposure to associated risks.

3. **Have you ever experienced any fraudulent activity while using internet banking? Response:** Yes (25%), No (40.9%), Not Sure (34.1%)

Analysis: A quarter of respondents reported experiencing fraudulent activity while using internetbanking.

Discussion: The prevalence of fraudulent activity highlights the importance of implementing robust security measures and educating users about safe online banking practices.

4. **Are you aware of the risks associated with internet banking?**

Response: Yes (27.3%), No (9.1%), Somewhat (63.6%)

Analysis: The majority of respondents have some awareness of the risks associated with internet banking.

Discussion: Despite a significant proportion indicating awareness, there is still a need for further education to enhance understanding of potential risks and how to mitigate them effectively.

5. **Have you taken any measures to protect yourself from internet banking fraud? Response:** Yes (18.2%), No (13.6%), Not Sure (68.2%)

Analysis: A majority of respondents are unsure whether they have taken measures to protect themselvesfrom internet anking fraud.

6. **What are the key determinants of your intention to continue using internet banking?**

Response: Perceived Usefulness (6.8%), Social Risk (11.4%), Time Loss Risk (25%), Opportunity Cost Risk

(0%), All of the Above (56.8%)

Analysis: Perceived usefulness is identified as the key determinant for continuing internet banking usage, followed by time loss risk.

Discussion: Understanding these determinants can inform strategies to enhance user satisfaction, trust,and retention in internet banking services.

7. Do you think enhanced security measures are necessary to prevent internet banking fraud? Response:

No (11.4%), Yes (81.8%), Not Sure (11.4%)

Analysis: The majority of respondents believe enhanced security measures are necessary to prevent internet banking fraud.

Discussion: This underscores the importance of continuous innovation and investment in securitytechnologies to safeguard users' financial information and transactions.

8. Do you think customer education and awareness programs are effective in establishing trust in online banking?

Response: No (13.6%), Yes (75%), Utmost Important (13.6%), Not Sure (4.5%)

Analysis: A minority of respondents perceive customer education programs as effective, while a majority consider them crucial.

Discussion: Effective education and awareness initiatives can empower users to make informed decisions and mitigate risks associated with internet banking.

9. What steps do you think banks, regulators, and policymakers should take to mitigate the risks associated with internet banking fraud?

Response: Implement Enhanced Security Measures (29.5%), Provide Customer Education and Awareness Programs (27.7%), All of the Above (45.5%), None of the Above (2.3%)

Analysis: Implementing enhanced security measures is identified as the primary step for mitigatingrisks, followed by customer education and ongoing research.

Discussion: Collaboration between stakeholders is essential to address evolving threats and ensurethe resilience of internet banking systems.

10. What are the suggested program areas for customer education and awareness programs?

Response: Online Purchasing (38.4%), Password Protection (40.9%), Debit/Credit Card Protection(21%)

Analysis: Respondents unanimously suggest focusing on online purchasing, password protection,and debit/credit card protection in customer education programs.

Discussion: Tailoring educational content to address specific areas of concern can enhance user engagement and effectiveness in promoting safe online banking practices.

Chapter 5:

Conclusion:

1. **Growing Concerns and Risks**: Financial services have been transformed by online banking, which not only provides unmatched ease but also raises serious concerns because of the always changing cyber threat scenario. Online banking fraud has gained considerable attention as a result of hackers taking advantage of flaws in digital environments, which affects both financial institutions and consumers.

2. **Need for Increased Awareness and Security Measures:** Financial institutions must take proactive security measures and increase consumer awareness of the growing threat of online banking fraud. It takes ongoing attention to detail and flexibility to respond to new threats in order to manage operational and security risks, such as transactional failures, data breaches, and unauthorized access.

3. **Impact on Trust and Reputation:** Fraud involving internet banking not only causes losses in money but also damages people's faith in financial institutions. To prevent long-term reputational harm and keep customers loyal, successful recovery plans and steps to restore consumer trust are crucial after fraud occurs.

4. **Importance of Regulatory Frameworks:** The implementation of regulatory frameworks is crucial in the fight against online banking fraud; however, additional study is necessary to evaluate the efficacy of current legislation and enforcement protocols. Enhancing fraud prevention and enforcement activities can be achieved by identifying holes in regulatory monitoring and putting targeted solutions into place.

5. **Opportunities for Future Research:** There are still unanswered questions in the field despite a great deal of research, such as the unique difficulties that users of online banking encounter in various geographical areas, the effect that fraud has on bank performance and customer satisfaction, and the efficiency of security and awareness campaigns. In order to successfully educate policy and practice and give more robust evidence, future research should employ quantitative approaches.

In conclusion, tackling the complex issues of online banking fraud necessitates a concerted effort from regulators and legislators to financial institutions and end users. The hazards of online banking fraud can be reduced, and customers' continuous faith and confidence in digital financial services can be guaranteed, by raising awareness, improving security protocols, and fortifying legal frameworks.

Recommendations:

1. **Quantitative Methodology:** To offer solid proof of the influence of online banking on bank performance and the growth of online banking in India, future studies had to take a quantitative approach. Researchers can learn more about user behaviors, attitudes, and experiences regarding online banking security and fraud by examining quantitative data.

2. **Identification of Particular Risks and Challenges**: Future research should concentrate on identifying particular risks and difficulties related to internet banking in India, along with suggesting focused measures to

reduce these risks. Effective methods to improve online banking security and fraud awareness can only be developed by taking into account the particular issues that banks and consumers confront.

3. **Distinguishing Between Fraudulent Acts:** In order to offer more focused suggestions for mitigation and prevention, future research should distinguish between distinct fraudulent acts. Through the analysis of scammers' various methods, researchers can create customized defenses against particular forms of online banking fraud.

4. **Evaluation of Regulatory Frameworks:** In order to prevent online banking fraud and increase public awareness, it is necessary to evaluate how well regulatory frameworks are working. Policymakers can pinpoint areas for improvement and enact stricter measures to protect online banking transactions by assessing the effects of current legislation and enforcement tactics.

5. **Emphasis on consumer Education Initiatives:** Scholar's ought to investigate how well consumer education and awareness initiatives contribute to building internet banking confidence. Through assessing how instructional programs affect user behaviors with expertise, stakeholders can improve already-existing programs and create focused interventions to raise consumer awareness of fraud.

References:

1 P. K. Gupta, P. K. (2008). Internet banking in India: consumer attitudes and futurechallenges. Internet Banking and Commerce, 13(2), pp. 1-15.

2 M. Vrincianu and L. A. Popa. (2010). Electronic banking security concerns: consumerprotection measures in Romania. 5(4), 446-460. Journal of Applied Quantitative Methods.

3 W. Nasri. (2011). Factors impacting internet banking uptake in Tunisia. Internet Banking and Commerce, 16(1), pp. 1-18.

4 R. Barker. (2011). A knowledge management strategy to managing online crisis communication responses in regard to illicit financial transactions. 1-7 in SA Journal ofInformation Management, 13(1).

5 R. Barker. (2011). Globalization, technology, and the banking industry: Opportunities andchallenges. 7(2), 57-67, Journal of Global Business and Technology.

6 Usman, A. K., and M. H. Shah (2011). Electronic Banking Fraud and Security Concerns in Developing Economies. 219-226 in International Journal of Business and Social Science, 2(13).

7 A. O. I. Hoffmann and C. Birnbrich (2012). Evidence from the German retail banking business on the quality of customer interactions and customer loyalty. 30(4), 282-298 inInternational Journal of Bank Marketing.

8 W. Wei, J. Li, L. Cao, Y. Ou, and J. Chen (2012). An effective approach for detecting online banking fraud through the use of data mining and profiling techniques. Decision Support Systems, vol. 54, no. 1, pp. 83-93.

9 A. Kesharwan and T. Tripathy (2012). An empirical study of perceived risk and internet banking usage in India. 30(4), 303-322, International Journal of Bank Marketing.

10 N. S. van der Meulen (2013). Who is in charge of internet banking fraud? 302-311 in Journal of Financial Crime, 20(3).

11 Mahmood Shah. "Key success factors for the prevention of fraud in e-banking systems." Journal of Money Laundering Control 16, no. 2 (2013): 168-182.

12 Rashidah, Abdul Rahman, and Irda Syahira Khair Anwar. "Fraud Detection and Prevention Measures in Malaysian Islamic Institutions." Journal of Financial Crime 21,no. 4 (2014): 423-437.

13 Dr. N. J. Uke and Samir Pakojwar. "Secure internet banking: vulnerabilities, attacks, and countermeasures." Journal of Information Security 5, no. 3 (2014): 67-87.

14 Martins, Carolina, Tiago Oliveira, and Ale Popovic are the players. UnderstandingInternet Banking Adoption and Use Behaviour: A Unified Theory of Acceptance and Use of Technology and Perceived Risk Application, 34, no. 1 (2014): 1-13.

15 Shewangu, Dzomira, and others. African Journal of Business Management, "Electronic fraud in the banking industry: Challenges and Solutions."

16 By Rodrigo Carvalho, "Ontology-Based Cybercrime Investigation Framework for Online Banking Fraud." Pages 62–67 of the Proceedings of the Seventh International Conference on Security of Information and Networks. 2014.

17 R. Carvalho. Using Semantic Technologies to Improve Cybercrime Investigations, Journal of Universal Computer Science, 21(10), 1261-1283.

18 Kassim, N. M., and T. Ramayah (2015). A Literature Review on Semantic Technologies for Cybercrime Investigations. Journal of Theoretical and Applied Information Technology, 80(1), pp. 101-113.

19 R. Abreu, F. David, M. Legcevic, L. Segura, H. Formigoni, and F. Mantovani. Ethics and Security Risks in E-banking Services: A Portuguese Case Study. Journal of Electronic Commerce Research, 16(2), pp. 130-145.

20 M. L. Bhasin. Bank Fraud in India: An Empirical Study, Journal of Financial Crime,22(1), pp. 4-19.

21 Al Zaabi, K., and A. Tubaishat (2015). Customers of E-banking might benefit from an information security awareness programme. International Journal of Cyber-Security andDigital Forensics, 4(1), pp. 13-22.

22 (2017) Alghazo, J. M., Kazmi, Z., and Latif. Internet banking security in developingnations: a client-centered strategy. 24(1), 105–119, Journal of Financial Crime.

23 S. Dzomira. Electronic Banking Services and Plastic Money: Raising Financial Identity Theft Fraud Risk Awareness in Zimbabwe's Banking Sector Through Bank Websites. Journal of Internet Banking and Commerce, 22(3), pp. 1-17.

24 R. Barker. E-banking Fraud Prevention Through Knowledge Management and Co- liability. International Journal of Information Management, 38(1), pp. 202-209.

25 P. van Schaik and J. Jansen. A Partial Least Squares Path-Modeling Approach to Understanding Precautionary Online Banking Behaviour. International Journal of BankMarketing, 36(5), 925-941.

26 O. M. Fadayo. E-banking Fraud Prevention and Detection: An Analysis of Issues Facedby Nigerian Financial Institutions. Journal of Financial Crime, 25(3), 695-709.

27 R. Barker (2018). Lessons from the South African Banking Risk Information Centre on Proactive Communication and Knowledge Management for E-Banking Fraud Prevention. 20(1), 1–9 of the South African Journal of Information Management.

28 I. Skula, J. Bohacik, and M. Zabovsky (2020). An exploratory study of channels and determinants in fraud prevention awareness efforts. 865-881 in the Journal of FinancialCrime.

29 I. Ahmad, S. Iqbal, S. Jamil, and M. Kamran (2021). E-banking system security: An in- depth examination of recent advancements and vulnerabilities. 102348, Computers & Security.

30 P. Sood and P. Bhushan (2022). Banking fraud in India: Data from the Central VigilanceCommission. 437-453 in Journal of Financial Crime, 29(2).