Global Scientific JOURNALS

GSJ: Volume 10, Issue 6, June 2022, Online: ISSN 2320-9186

www.globalscientificjournal.com

INTERNAL CONTROL MEASURES ON FRAUD DETECTION AND PREVENTION IN FINTECH COMPANIES IN KENYA

Doughty Natalie Wanyama[a], Dr. James Mwikya Reuben[b]

[a]Management University of Africa, P.O Box 29677-00100, Nairobi Kenya

[b]Kirinyaga University, P.O.Box: 143-10300, Kerugoya, Kenya

[a]doughtynatalie7@gmail.com,

[b]jmwikya@kyu.ac.ke;

ABSTRACT

The study sought to examine the effect of internal controls on fraud detection and prevention among Financial Technology (FINTECH) Companies in Kenya, case of Interswitch (Kenya) Limited. The study adopted three major objectives; to establish the impact of know your customer practices on fraud detection and prevention, to examine the effects of information technology on fraud detection and prevention and to determine the impact of staff training on fraud detection and prevention. The target population of 200 and a sample size of 100 people, this study employed primary data collected through questionnaires. The study adopted a descriptive survey research design, the decision to apply descriptive cross-sectional survey research design. The study results showed R = 0.734 that means there was strong and positive relationship between the study's internal control measures and fraud detection and prevention. Further the regression shows an overall R^2 = 0.539 meaning that 53.9% of the measures of detection and prevention of fraud in financial technologies companies in Kenya is explained by the three independent variables namely information technology, know your customer and staff training. Study conclusions are; through reliable information technology, company management will be able to take strategic decisions for the future of the company, especially in detection and prevention fraud. The use of CAATs or e-audit systems is able to overcome fraud risk and this is believed to be able to detect the possibility of fraud that may occur. Know your customer check should be a mandatory process of identifying and verifying the client's identity when opening an account and periodically over time. In order to detect and prevent fraud, employees must first know what to look for, and then what to do about it. Finally the internal control measure's has an influence on detection and prevention fraud.

Keywords: Internal Control, Detection and Prevention, Fraud, Fintech

INTRODUCTION

As the world economy continues to globalize and competition increase the key challenge of today's economy is how to prevent and detect fraud amidst the upsurge of use of technology to transact globally. It is because of this business evolution that financial technology (Fintech) is the most popular trend across the globe. Fintech is used to describe how technology is utilized by companies to deliver their customer's financial products and services. It is a combination of "Financial" and "Technology", and the major areas of business that Fintech is utilized include banking, investing, insurance, lending, and anything that has to do with finances. Innovation in financial technology is rapidly transforming the global financial sector. Since 2010, more than US$50 billion has been invested in almost 2,500 companies worldwide as FinTech redefines the way in which we store, save, borrow, invest, move, spend, and protect money (Skan, Dickerson, and Gagliardi 2016).

Fintech is changing perception on finances and money in general, as now one can open a Bank account; deposit and withdraw cash via mobile and check the account balance; make payment for shopping from stores and other POS machine outlets like filling station. One of the great advantage of Fintech is that companies do not require to invest in physical infrastructure for example branches thus consumers benefiting access to cheaper deals and walking around safely without necessarily having to carry hard cash but rather e- wallets but now having to deal with the disadvantages fraudulent activities that comes with the use of technology. The Fintech industry has had a great deal to celebrate – a recent report by KPMG International and CBK Insights, suggested a record US$19.1 billion was raised across 1162 deals last year globally, and innovation has been rapid and impressive, bringing new products to a well-established and traditional sector. There is another side to this industry disruption, however, which is the heightened risk of fraud. Recent fraud-related scandals involving peer-to-peer and crowd funding platforms have served as stark reminders of the risks of using FinTech when appropriate regulation and/or compliance processes are not in place. Users of FinTech are concerned about

fraud, so for the FinTech industry to survive, it must be protected against exploitation by fraudulent activity. (Glass & Agarwal, 2016;Ferrari, 2016).

Currently in Kenya as the information age progresses, there is increase in technological progress thus fostering free flow of ideas and knowledge across the nation and global interaction. From an organizational standpoint, the information age is in full swing and both public and private institutions are experiencing an increase in the use of a variety of information technologies (IT's). Unfortunately, with this rapid adoption and expansion of the fintech industry comes issues of fraud and security for the market sector. Fintech organizations are in the jurisdiction of IT industry and therefore the internal control measures of detection and prevention of fraud plays a key role in the protection and even the continuity of the business (Mwikya & Obura, 2021). The components of internal control include measures of detection and prevention of fraud include but not limited to control environment, risk assessment, control activities, information and communication technology, knowing your customer, daily reconciliations, staff training, checks and controls, and supervision (COSO, 2013; Fourie & Ackermann, 2013). Fraud detection and prevention often requires a variety of technologies and even being on the lookout for any emerging trends that could be a threat to the Fintech company.

Staff training is a programme executed by a manager or a person of authority to equip specific staff members with the necessary skills and knowledge required to perform a specific role. Eaton and Korach (2016) opined that understanding behavioral aspects helped to prevent fraud. Specifically, the behavioral aspects of personality characteristics, psychology, and sociology showed the aspects involve in occupational fraud. Further knowing your customer in financial services, require that professionals try to verify the identity, suitability and risks involved with maintaining a business relationship. Fraud deterrence are measures to stop fraud occurring in the first place, whereas fraud detection involves identifying fraud as quickly as possible once it has been perpetrated (Naicker, 2006; Kabue and Aduda, 2017). The system of knowing your customer should emphasize on, proper identification measurement and monitoring of risks, control activities for each level of operation, creation of reliable information systems that promptly reports anomalies and detailed reporting of all operations and monitoring of all the activities (Opromolla & Maccarini, 2010; Mustafa and Youssef, 2010) stated that information technology includes computers, software, databases, networks, electronic commerce, and other types of technology-related types. Information technology uses computer technology for

processing and storage, also functions as a communication technology for dissemination. The application of good information technology can also guarantee the quality of financial statements. This is because the use of information technology can accelerate financial information that is updated in a short time. Hence the better the technology used, the better the quality of financial reports.

Interswitch East Africa (Kenya) Limited is a Payments Service Provider (PSP) company, duly licensed by the Central Bank of Kenya (CBK). Focused on Financial Technology, Interswitch aims at securely enabling the circulation of money through Transaction Switching and Processing, Digital Payments and E-Commerce. It is one of the companies that fall under the umbrella Interswitch Group of Companies. Interswitch group provides advisory services, technology integration, digital commerce and digital payment solutions with the aim of promoting fast, innovative and secure payments and transaction technology to all Africans thus play its part in providing faster economic growth in all of Africa.

1.1 Statement of the problem

People all over the world are rapidly adopting fintech solutions. In fact, the global fintech market will reach an estimated $190 billion by 2026, growing at 13.7% Compound annual growth rate. Unfortunately, this increase, and increased frequency of digital transactions, has led to higher rates of fraud occurrence and loss. The reality is that due to constant changes in technology and the increase in frequency and the volume of digital transactions, companies are not always fully equipped to prevent fraud. This is often because current fraud prevention techniques are rooted in manual detection, meaning that before a company can implement preventative measures, a form of fraud must be detected by an individual. The regularity of fraud and misappropriation of funds is creating fear, anxiety, and a loss of confidence in the minds of fintech customers. Management is required to set up an internal control system but this system varies significantly from one organization to the next, depending on such factors as their size, nature of operations, and objectives. Since internal controls operate in an environment which influences its operations, proper care must be exerted into the implementation of these systems in order to achieve the utmost aim of the fintech. This study sought to examine the effect of internal controls on fraud detection and prevention among financial technology (fintech) companies in Kenya, case of Interswitch (Kenya) Limited.

1.2 Study Objectives:

(i) To examine the effect of information technology on fraud detection and prevention.

(ii) To establish the influence of know your customer practices on fraud detection and prevention

(iii) To determine the influence of staff training on fraud detection and prevention and prevention

LITERATURE REVIEW

2.1 Theoretical Framework

2.1.1 Theory of Internal Control

A system of effective internal control is a critical component of an organization's management and a foundation for its safe and sound operation. A system of strong internal control can help to ensure that the goals and objectives of an organization will be met, that it will achieve long-term targets and maintain reliable financial and managerial reporting. Such a system can also help to ensure that the organization will comply with laws and regulations as well as policies, plans, internal rules and procedures, and reduce the risk of unexpected losses and damage to the organization's reputation. The following presentations of internal control in essence cover the same ground. In USA, the Committee of Sponsoring Organizations of the Tread way Commission (COSO) issued Internal Control – Integrated Frame working 1992, which defined internal control as a process, effected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories: Effectiveness and efficiency of operations; Reliability of financial reporting; Compliance with applicable laws and regulations. The Rutteman Report (1994) in UK defined internal control as the whole system of controls, financial and otherwise, established in order to provide reasonable assurance of Effective and efficient operations; Internal financial control and Compliance with laws and regulations. The theory is relevant to the study because it outlines the internal control policies, procedures and rules to be followed in the banking industry.

2.1.2 The technology acceptance model

The technology acceptance model (TAM) is an information system theory that seeks to explain using a model, the acceptance and use of a technology by users' (Davis, 1989). TAM is used to explain the acceptance of a new technology in the work place and which users are likely to embrace the new technology. Two major factors inform the user's decision on the use of the new technology and this include; perceived usefulness, this is the extent to which an individual believes that using a particular system would complement their job performance and perceived

ease of use, which is the extent to which an individual believes that using a particular system would be effortless. Continuous studies on the model have resulted in new versions such as the unified theory of acceptance and use of technology (UTAUT) and TAM 2 (Venkatesh; Viaswanath and Davis; Fred D., 2000). TAM has been useful in explaining various system use such as online system which include electronic Learning systems, information management systems and web-based applications as noted by (Fathema, Sutton, 2013, Fathema, Shannon, Ross, 2015, Fathema, Ross, Witte, 2014).

2.2 Empirical Literature Review

Devaraj and Kholi (2003) that information technology has a significant role for the future of the company. Furthermore, Wilkinson and Cerullo (1997) stated that good information technology will provide accurate information and this can minimize fraud. In line with Elder et al (2013) states that sophisticated information technology in entities is able to assist management in segregating employee duties so that opportunities for asset misappropriation can be minimized. Advanced information technology can be realized by management with the use of accounting applications that are able to assist entities in business management. One example is e-procurement, an information technology system used to procure goods. So far this system is considered the best to minimize fraud in the procurement of goods (Oktaviani, 2017). In addition, according to Olasanmi (2013) stated that the use of CAATs or e-audit systems is able to overcome fraud risk and this is believed to be able to detect the possibility of fraud that will occur.

According to International Monetary Fund, (2018) Cyber-threats have been identified as a major challenge because of the potential systemic risks and interaction with other risks. Despite these cyber-threats, start-up fintech firms are unable to implement expensive cyber security detection and prevention applications which might be overkill, both financially and functionally. A possible cause of this problem is limited domain knowledge about the types of threats and capability of analysing the possibility of threats and narrow knowledge on functional and least costly tools for detection and prevention of cyber-threats (mwikya&obura,2021). The common cyber-threats to fintechs startups are Malware, distributed denial of service (DDoS) and Botnets, Web Application attacks and System Vulnerabilities threats. The study identified several open-source applications for detection and prevention of these cyber-threats and recommends the following applications; Chkrootkit,ClamAV, NeoPI, CrowdSec, Suricata, SNORT, Grabber,

SQLMap, Wapiti, Nessus, Sn1per andNettacker. The study suggests further research on fifth generation architectures cloud computing, Internet of Things and Artificial Intelligence for detection and prevention of cyber-threats (mwikya&obura,2021).

According to Thales (2022), Know Your Customer (KYC) is today a significant element in the fight against financial crime and money laundering, and customer identification is the most critical aspect as it is the first step to better perform in the other stages of the process. Know your customer is a key compliance issue, whereby an institution is required to identify all the features of its clients by updating existing files and monitoring the operations and checking at least that originators and beneficiaries are not blacklisted (Hardouin, 2009). The global anti-money laundering (AML) and countering the financing of terrorism (CFT) landscape raise tremendous stakes for financial institutions. KYC means Know Your Customer and sometimes Know Your Client. KYC or KYC check is the mandatory process of identifying and verifying the client's identity when opening an account and periodically over time. In other words, banks must make sure that their clients are genuinely who they claim to be. Banks may refuse to open an account or halt a business relationship if the client fails to meet minimum KYC requirements. KYC procedures defined by banks involve all the necessary actions to ensure their customers are real, assess, and monitor risks. These client-on boarding processes help prevent and identify money laundering, terrorism financing, and other illegal corruption schemes. KYC process includes ID card verification, face verification, document verification such as utility bills as proof of address, and biometric verification. Banks must comply with KYC regulations and anti-money laundering regulations to limit fraud. KYC compliance responsibility rests with the banks. In case of failure to comply, heavy penalties can be applied (Thales 2022).

According to TowneBank (2022), most fraudulent activity can be caught by putting effective internal processes and procedures in place to minimize the chances for illegal behaviour. Staff training is a key element in risk management as employees who are actively trained in risk management are better able to identify threats to the organization due to weak or non-existent internal controls (Rae & Subramaniam, 2008). But don't forget one of the best sources of fraud prevention: your employees. In order to detect and prevent fraud, employees must first know what to look for, and then what to do about it. Employee fraud can take place in many ways, but by far the most common involves accounting, accounts payable, and payroll functions. In order to commit fraud, it helps to have access to money and accounts. Employees who submit

expenses reports are also prime sources of fraud, especially if your internal controls are weak. Internal training should include: Create separate duties with checks and balances built in. Require multiple approvals for expenditures. Have multiple employees keep the books, handle payroll, make deposits, and reconcile bank statements. Cross-train employees to perform basic financial functions. Relying on one person to handle a financial process makes it easier for that person to commit fraud. Train employees to perform basic internal audits – outside of their normal work area. Oversight is a great deterrent. Then focus on training employees to identify external sources of fraud, including identity theft. each employees to watch for: New account fraud – setting up accounts based on stolen identity or personal information, Credit card fraud – using credit cards without authorization, Check fraud – using checks without authorization, or using fake checks, Phishing – fraudulent attempts to get personal or company information that can be used to perpetrate identity theft, Identity theft – using another individual's personal or financial information without his or her consent, Invoicing for products or services that were never provided, Invoicing for over-utilization of services that is billing for unneeded services; the services were performed but were not needed or requested and Kickbacks (TowneBank, 2022).

RESEARCH METHODOLOGY

3.1 Research Design

The study adopted a descriptive survey research design. The researcher applied this design to evaluate the impact of internal controls on the detection and prevention of fraud in Interswitch East Africa (K) Limited. This design was very useful in studying the inter-relations between the variables already mentioned in the conceptual framework (Churchill & Iacobucci, 2010). The decision to apply descriptive cross-sectional survey research design was based on the fact that in the study, the researcher’s interest was on the state of affairs already existing in the field and that no variable is to be manipulated. Descriptive cross-sectional survey designs are used in preliminary and exploratory studies to allow researchers to gather information and summarize, present and interpret data for the purpose of clarification (Sekaran and Bougie, 2010). The design was chosen for this study due to its ability to ensure minimization of bias and maximization of reliability of evidence collected.

3.2 Target Population

The population of the study comprise of the entire Interswitch East Africa (k) ltd operating in Kenya in terms of card services, ATM and PO’s management services, corporate payments and bill payment that sums up to a target population of 200.

3.3 Sample and Sampling Technique

The researcher picked a representative sample of the whole population from staff inventory. To achieve a representative sample for a research study, the people who were studied (i.e., the subjects) were carefully selected using a simple random sampling methods Amin (2005).

Table 1: Sample and Sampling Technique

Population category	Sample Target	Percentage (50%)
Mangers	17	17
Supervisors	34	34
General staff	49	49
Total	**100**	**100**

3.4 Data Collection Instruments

The questionnaires that were used to collect data at Interswitch in relation to internal control measures and the measures put in place to detect and prevent fraud in Interswitch East Africa (K) Limited.

3.5 Reliability and Validity of the Study

Reliability denotes to the uniformity or rather the dependability of the scores that were attained from tests and valuation procedures. Mugenda and Mugenda (2013) argued that accountability may be animate to the degree of the researchers' instrument yields being consistent with the results once recurrent trials were conducted. This study adopted test-retest that involved administering the form at intervals of one week as a pilot takes a look at two identical cluster to examine two scores. Validity refers to whether a questionnaire is measuring what it purports to measure (Heale&Twycross, 2015). To ensure content validity, the questionnaire was subjected to a thorough examination by supervisors in charge of the study development. They were asked to evaluate the statements in the questionnaire for relevance. Based on the evaluation, the instrument was adjusted appropriately before subjecting it to the final data collection exercise. Their review comments were used to ensure that content validity is enhanced.

STUDY FINDINGS AND DISCUSSION

4.1 Demographic Information

Employees of Interswitch East Africa (K) Limited participated in this study. A sample size of 100 was obtained using random sampling technique. A total of 100 questionnaires were distributed. Out of the 80 questionnaires received, 10 were rejected owing to missing information/incomplete responses. The complete forms were 70 representing 70% of the entire administered questionnaires. The results shows that 44% of respondents were male while female

were 56% of the participants. Participants in the age groups; 20–30, 31–40, 41–50, and 51–6 age groups, accounted for 30%, 40%, 20%, and 10%, respectively. Similarly on the highest level of qualification of the respondents, 20% participants had certificate, 35%of the participants had diploma, 40% of the participants had bachelor's degrees, and 5% of the participants' Postgraduate degree. On the work experience, 35% of the participants had less than 1 year of work experience, 45% participants had 1–5 years and 20% had more than 10 years of work experience (Table2).

Table 2: Demographic Information

Controls		**Variance (%)**
Gender	Male	44
	Female	56
Age	20-30 years	30
	31-40 years	40
	41-50 years	20
	51-60 years	10
Education	Certificate	20
	Diploma	35
	Degree	40
	Postgraduate	5
Work Experience	0-5 years	35
	6-10 years	45
	Above 10 years	20

4.2 Correlation analysis

The study first determined the relationships among the study variables. The association between the internal control measures and fraud detection and prevention in fintech companies in Kenya were determined through correlation coefficient. The relevant results are presented in table 3.

Table 3: Correlation of the study Variables

		Detection and prevention	Information Technology	Know your Customer (KYC)	Staff Training
Detection and prevention	Pearson Correlation	1	.485**	.468**	.265**
	Sig. (2-tailed)		0	0	0.007
Information Technology	Pearson Correlation	.485**	1	.477**	0.137

		Detection and prevention	Information Technology	Know your Customer (KYC)	Staff Training
	Sig. (2-tailed)	0		0	0.168
Know your Customer (KYC)	Pearson Correlation	.468**	.477**	1	.402**
	Sig. (2-tailed)	0	0		0
Staff Training	Pearson Correlation	.265**	0.137	.402**	1
	Sig. (2-tailed)	0.007	0.168	0	

***. Correlation is significant at the 0.01 level (2-tailed); N=70*

The results in Table 3 show that the association between information technology is highly correlated with fraud detection and prevention (r =.485 and P<0.05). This is a positive and strong correlation coefficient implying that there exists a strong relationship between information technology and fraud detection and prevention that is statistically significant. This was followed by correlation between Know your Customer (KYC) and fraud detection and prevention (r =.468 and P<0.05), a high correlation value above 0.5 indicating that Know your Customer (KYC) is positively correlated to fraud detection and prevention and p-value of below 0.05 indicates that the relationship is statistically significant. Finally, Staff Training and fraud detection and prevention (r=.265 and p-value<0.05) implying a statistically significant relationship and the association is medium. This can be interpreted to mean that internal controls; Information Technology, Know your Customer (KYC) and Staff Training play a big role towards fraud detection and prevention in fintech companies in Kenya.

4.3 Regression Analysis

Regression analysis was conducted to establish the relationship between the internal control measures with prevention and detection of fraud in fintech companies in Kenya.

Table 4: Model Summary

Model	R	R Square	Std. Error of the Estimate
1	.734[a]	.539	.02031

According to the table 4 above, the regression analysis shows an overall relationship of R = 0.734 and R^2 = 0.539 of the three independent variables that were studied, only 53.9% of the measures of detection and prevention of fraud in financial technologies companies in Kenya is explained by the three independent variables (Information Technology, Know your customer

(KYC) and Staff Training) which are represented by the R^2. Therefore, this means that other factors not captured within the scope of this study subsidizes the remainder of 46.1% hence further research should be conducted to investigate those factors. The above model is well-thought-out since R^2 greater than 50% which is considered viable. Therefore the results of the findings above revealed that the level of significance was P<.000 this implies that the regression model is significant in predicting the relationship between the internal control measures and the detection and prevention of fraud in fintech companies in Kenya and in this case Interswitch East Africa (K) Limited.

Table 5: ANOVA

Model	Sum of Squares	df	Mean Square	F	Sig
Regression	38.403	3	12.801	26.893	0
Residual	32.822	69	0.476		
Total	71.225	70			

The values of F = 26.893 show that all the predictor factors statistically and significantly affect detection and prevention of fraud in fintech companies in Kenya, which means the regression model is a good fit of the data and internal control measures significantly influences detection and prevention of fraud in in fintech companies in Kenya. The level of significance is 0.000 which is less than 0.05 hence the overall regression model significantly predicts the dependent variable. The results were enumerated as seen in Table 5.

Table 6: Coefficients

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	95.0% Confidence Interval for B	
		B	Std. Error	Beta			Lower Bound	Upper Bound
	Constant	0.348	0.315		1.106	0.271	-0.276	0.973
	Know your customer(KYC)	0.179	0.085	0.186	2.116	0.037	0.011	0.347
	Information Technology	0.553	0.077	0.596	7.14	0.000	0.399	0.706
	Staff Training	0.101	0.06	0.128	1.978	0.047	0.018	0.221

a. Dependent Variable: detection and prevention

The study outcome indicated that the predictor variables have a significant positive impact on detection and prevention of fraud in fintech companies in Kenya. The results indicate that there is significant relationship between the internal control measures and

detection and prevention of fraud in fintech companies in Kenya; $p < 0.05$ ($P = 0.01$). Thus, the values of predictor variables are statistically significant with $p < .05$ which means an increase in mean index of predictor variables will increase detection and prevention of fraud. Therefore, the optimal regression model for the study is:

Detection and prevention of fraud = 0.348 + 0.179 (Know your customer) + 0.553 (Information Technology) +0.101 (Staff Training)

The model shows that Information technology was the predictor variable that highly affected detection and prevention of fraud in financial technologies companies in Kenya, followed by Know your customer. Staff Training had the least effect on detection and prevention of fraud. The results were enumerated as seen in table 6.

SUMMARY AND CONCLUSIONS

5.1 Summary

The results on the study objective shows that the association between information technology is highly correlated with fraud detection and prevention ($r = .485$ and $P<0.05$). This is a positive and strong correlation coefficient implying that there exists a strong relationship between information technology and fraud detection and prevention that is statistically significant. Information technology is important in fraud prevention. Through reliable information technology, company management will be able to take strategic decisions for the future of the company, especially to avoid fraud. This is consistent with the opinion of Devaraj and Kholi (2003) that information technology has a significant role for the future of the company and that the use of CAATs or e-audit systems is able to overcome fraud risk and this is believed to be able to detect the possibility of fraud that will occur. Additionally the study results shows that there is correlation between Know your Customer (KYC) and fraud detection and prevention ($r = .468$ and $P<0.05$), a high correlation value above 0.5 indicating that Know your Customer (KYC) is positively correlated to fraud detection and prevention and p-value of below 0.05 indicates that the relationship is statistically significant. This is consistent with Thales (2022) who opined that KYC check should be a mandatory process of identifying and verifying the client's identity when opening an account and periodically over time. Further the study results showed that staff training and fraud detection and prevention had a correlation of ($r=.265$ and p-value<0.05) implying a statistically significant relationship and the association is medium. This conforms to TowneBank (2022) that in order to detect and prevent fraud; employees must first know what to look for, and then what to do about it.

Finally the regression analysis shows an overall relationship of R = 0.734 and R^2 = 0.539 of the three independent variables that were studied, 53.9% of the measures of detection and prevention of fraud in financial technologies companies in Kenya is explained by the three independent variables (Information Technology, Know your customer (KYC) and Staff Training). Therefore, this means that internal control measures affects detection and prevention of fraud in financial technologies companies in Kenya. The other factors not captured within the scope of this study subsidizes the remainder of 46.1% hence further research should be conducted to investigate those factors.

5.2 Conclusions

Through reliable information technology, company management will be able to take strategic decisions for the future of the company, especially in detection and prevention fraud. The use of CAATs or e-audit systems is able to overcome fraud risk and this is believed to be able to detect the possibility of fraud that will occur. Know your customer check should be a mandatory process of identifying and verifying the client's identity when opening an account and periodically over time. In order to detect and prevent fraud, employees must first know what to look for, and then what to do about it. Finally the internal control measure's has an influence on detection and prevention fraud.

References

Aware, Inc (2022) https://www.aware.com/blog-high-fraud-rates-fintech-prevention-methods/

Davis, F. D. (1989) 'Perceived usefulness, perceived ease of use, and user acceptance of information technology', MIS Quarterly: Management Information Systems, 13(3), pp. 319–339. doi: 10.2307/249008.

Devaraj, S. and Kohli, R. (2003). "Performance Impact Of Information Technology: Is Actual Usage The Missing Link? "Management Science.

Eaton, T. V and Korach, S. (2016) 'A Criminological Profile', Journal of Applied Business Research, 32(1), pp. 129–142.

Fathema, N., Ross, M. and Witte, M. M. (2014) 'Student acceptance of university web portals: A quantitative study', International Journal of Web Portals, 6(2), pp. 42–58. doi: 10.4018/ijwp.2014040104.

Fourie, H. and Ackermann, C. (2013) 'The impact of COSO control components on internal control effectiveness: An internal audit perspective', Journal of Economic and Financial Sciences, 6(2), pp. 495–518. doi: 10.4102/jef.v6i2.272.

Juan Pablo Calle,(2020) https://www.piranirisk.com/blog/3-tools-for-monitoring-unusual-transactions

Kabue, L. N. and Aduda, J. (2017) 'Effect of Internal Controls on Fraud the Detection and Prevention Among Commercial Banks in Kenya', European Journal of Business and Strategis Management, 2(1), pp. 52–68. Available at: https://www.iprjb.org/.

Mustafa, S. T. and Ben Youssef, N. (2010) 'Audit committee financial expertise and misappropriation of assets', Managerial Auditing Journal, 25(3), pp. 208–225. doi: 10.1108/02686901011026323.

Mwikya Reuben and, Obura Johnmark (2021). KyU 4th Annual Virtual International Conference, 2021. Detection and Prevention of Cyber-threats using Open-Source Software for Fintech Startup Firms in Kenya.

Skan J, Dickerson J and Masood S (2016) The Future of Fintech and Banking: Digitally disruptedorreimagined?(availableat http://www.fintechinnovationlablondon.co.uk/media/730274/ Accenture-The-Future-of-Fintech-and-Banking-digitallydisrupted-or-reima-.pdf)

Thales (2022), https://www.thalesgroup.com/en/markets/digital-identity-and-security/banking-payment/ issuance/id-verification/know-your-customer

The Committee of Sponsoring Organizations of the Treadway Commission (COSO). (2013). Internal ControIntegrated Framework: Executive Summary. Durham:North Carolina.

TowneBank.(2022),https://www.townebank.com/business/resources/security/training-employees/

Venkatesh; Viaswanath and Davis; Fred D. (2000) 'A Theoretical Extension of the Technology Acceptance Model: Four Longitudinal Field Studies', Management Science, 46(2), pp. 186–204. Available at: https://www.jstor.org/stable/pdf/2634758.pdf.