Perceived Security of E-Payment System and Reduction in Incidence of Fraud in Kwara State Internal Revenue Service, Nigeria

A.E. Adeyemi[1], E. O. Dunmade[2] & C. K. Daramola[3]

[1&3] Department of Business Administration, University of Ilorin, Kwara State
[2] Department of Industrial Relations and Personnel Management,
University of Ilorin, Kwara State
NIGERIA
awadex4queen@gmail.com[1], dunmade.eo@unilorin.edu.ng[2],
daramolacomfort@gmail.com[3]

Abstract

Globally, governments have been embracing e-payment system to fast-track revenue collection, and to equally minimize incidence of fraud. However, a major threat to the smooth operation of e-payment in Nigeria is security related issues. Therefore, this study examined perceived security and incidence of fraud, with particular reference to Kwara State Internal Revenue Service (KWIRS), Nigeria. The study obtained a sample of 285 from a population of 996. The findings demonstrated that perceived security dimensions strongly contributed to reduction in incidence of fraud. The study concludes that improvements in e-payment system security, particularly with regard to trust issues, have a significant impact on the amount of fraud reduction in KWIRS. It is recommended that the government ensure the expansion of the country's e-payment system, which necessitates adequate collaboration with the private sector in expanding the existing internet facilities, in order to improve the convenience of use and safety for users.

Keywords-: Incidence of fraud, Perceived Level of Confidentiality, Perceived Level of Risk, Perceived Security, Perceived Trust

1. INTRODUCTION

Collection of revenue remains an important statutory activity for every government in the world that aims at developing her economy as it helps in the acquisition of resources not liable to debts (Ngotho & Kerongo, 2014). Past studies have however shown that most government face serious challenges in their revenue collection performance exercise (Balunywa, et al., 2014); which consequently result in government's inability to garner in sufficient funds to meet up with performing their statutory obligations. One of the major reasons for this is fraud, which is evidence, in that for

several years, revenue collection officials, have not been channeling all the amount of money collected to the government treasury (Ngotho & Kerongo, 2014).

Additionally, there have been cases of revenue collection officials conniving with tax payers to avoid the prescribed official charges and instead bribe their way to enable the collectors shield them against paying the correct amount to the government treasury. The resultant effect of such acts do dovetailed into a huge loss on the part of government, consequently

hampering economic development and improved service delivery. This therefore require the burning needs to eliminate or at least significantly reduce the incidence of fraud and corruption, by developing sound and simplify payment system that promote sure accountability for government establishments. Consequently, this has led to the adoption of electronic payment system (EPS) in public establishments, so as to facilitate critical changes in revenue transaction system (Njanja, 2014).

Essentially, adoption of e-payment system has been on the significant increase in the public institutions and business establishments. However, even with all the benefits associated with the system, fear of security breach, inadequate know-how among users, coupled with concerns over trust issues related to e-payment method of transaction remain serious concerns to individuals, organizations and experts in determining users' readiness to use e-payment. Nigeria is not an exempted from the aforementioned challenges.

In Nigeria, there are fundamental discouraging factors associated with adoption and successful operation of e-payment system as medium of basic transactions for government institutions. One of such threats is the fear of insecurity and trust. Obviously, using electronic payment system as a medium of basic transactions is subjected to security infringements such as stealing of commercially sensitive information; denial of service as a result of system errors, internet related frauds; leading to security infringements.

Government officials equally use the porous security system by conniving with computer hackers to steal from the coven of government treasury, thereby reducing the validity of the system, and consequently people's trust in government as an institution of change. Therefore, it is required that more attention be paid to the payment methods being provided to users (Antinoja & Scherling, 2019). This is pertinent because providing adequate security for e-payment process being used by government institutions is not only essential to the consumers who are revealing private and sensitive information about themselves on transaction but also to the institutions (Antinoja & Scherling, 2019; Fianyi, 2015).

Interestingly, across various countries and business organizations, e-payment system has been researched with increasing interest among many scholars and practitioners (Oney, Guven, & Rizvi, 2017). Nigeria with particular reference to Kwara State specifically provides an interesting case for the exploration of perceptions of field employees' in relation to perceived security of e-payment system. This is because the state is currently incorporating its governmental agencies, organisations and establishments, to an electronic system and, more importantly, an increasing number of Nigerian businesses are integrating EPS to their daily transactions.

The individual experiences of e-payment system' users in Nigeria are essential as they provide insights which, besides enriching the relevant literature, would offer a lucid perspective for practitioners such

government ministries, agencies and parastatals, as well as businesses and financial institutions that are currently using e-payment methods for basic transactions. Unlike the majority of the extant literature, this study primarily examines the nexus between fundamental factors associated with the issue of trust and security of e-payment system usage, from the standpoint of public employees, and its attendant effect on reduction in incidence of fraud, with the aim of providing a platform for enhancing public sector performance.

In the light of the foregoing, the specific objectives were to;

(i) Determine the extent to which social recognition and reputation of the company providing the e-service significantly influence incidence of fraud in Kwara State Internal Revenue Service (KWIRS);

(ii) Evaluate the effect of perceived level of risk-security in e-payment system on incidence of fraud in Kwara State Internal Revenue Service (KWIRS);

(iii) Examine the effect of perceived level of confidentiality on incidence of fraud in Kwara State Internal Revenue Service (KWIRS); and

iv) Investigate the extent to which perceived level of trust significantly influence incidence of fraud in Kwara State Internal Revenue Service (KWIRS).

1.2   Literature Review

1.2.1   Perceived Security of E-Payment System

Tsiakis and Sthephanides (2005) described system security as 'a set of

procedures, mechanisms and computer programmes to authenticate the source of information and guarantee the integrity and privacy of the data. The essence of this is to abstain from circumstance that could lead to mismanagement (economic) of data resources' (Oney, et al., 2017). According to Hartini, et.al (2020), security of e-payment system is the relevant procedures put in place to ensure prevention against an unauthorized or unlawful modification or destruction of information, which includes accidental and deliberately exposition of protected data. Thus, Fang, Chan, Brzezinski and Xu (2005) refer to perceived security "as the degree to which a user believes that using a particular application will be risk-free".

Invariably, perceived security e-payment system refers to the user personal view on the protection or safeness of a system (Hartini, et.al 2020; Hassan, Shukur & Hasan, 2020; Kim, Tao, Shin, & Kim, 2010). Flavian et al., (2006) described perceived security as a subjective probability with which users believe that their personal information (private and monetary) would not be viewed, stored, or manipulated during transit and storage by inappropriate parties in a manner consistent with their confident expectations. This translates to the technical aspects that ensure the integrity, confidentiality, authentication and non-fraudulent of transactions (Aziza, 2019).

According to Adeyinka (2012), the security dimension applies to issues relating to the security breach of the e-payment system, such as data theft,

which could increase in proportion to the number of users storing their personnel files on the system portal. In general, people would not be encouraged to use e-payment system if there were security or data breaches (Hartini, et.al 2020), and in which they perceived that the level of perceived security is too low (Masihuddin, Khan, Mattoo & Olanrewaju, 2017). Thus, it is imperative for system developer to provide detailed security policy statements, data protection, and privacy statements in order to assure users of their safety (Barkhordari et al., 2017).

1.2.2   Incidence of Fraud

Fraud has been one of the most challenging and unsolvable issues for many organized institutions all over the world. Thus, there have been much more attention and research dedicated to the topic, particularly, after the scandals such as Enron, WorldCom and host of others (Olaoye & Dada, 2017). Relating this to Nigeria, Almajir and Usaini (2020); Gbegi and Adebisi (2014) lamented that the level of fraud in the present day Nigeria has assumed an epidemic dimension. According to Ogbeide (2018), fraud is a social malady; keeping its perpetrators enriched and sometimes elevated in the inter-temporal period it occurs. It however often causes pains and frustration through losses and economic retrogression to the victims, be it individual, corporate bodies, or nations at large (Odukoya & Samsudin, 2021; Ogbeide, 2018).

Contextually, there is no universal definition of the term 'fraud' (Enofe,

et.al., 2015; Olaoye & Dada, 2017). However, looking at fraud from the legal point of view indicates that it is a generic term which involves different means human inventiveness can devise and which are resorted to by one individual or group of individuals to get an undue advantage over another by false pretences (Nigerian Criminal Code, 1990).

Economic and Financial Crime Commission (EFCC) Act (2004) defines fraud as illegal act that violates existing legislation and these include any form of fraud, trafficking narcotic drug, money laundering, bribery, embezzlement, looting and any form of corrupt malpractices and child labor, illegal oil bunkering and illegal mining, tax evasion, foreign exchange malpractices including counterfeiting currency, theft of intellectual property and piracy, open market abuse, dumping of toxic wastes and prohibited good, etc. The EFCC definition of fraud is all encompassing as it gives operational definition of fraud in corporate organizations and beyond (Udeh & Ugwu, 2018). Thus, necessary elements of fraud include unlawfulness, misrepresentation (which could be in the form of words, conduct, or failure to disclose); prejudice (which could either be actual or potential), and intention (Zachariah, et al., 2014).

Consequently, the common denominator of almost all the definitions point to the fact that fraud vary widely in nature, character, degree, and method of perpetration. Thus, the underlining and unique issue to the definitions is that the concept has been associated with

financial misappropriation and misstatement, political and economic corruption, identity theft, network hacking, concealment of material fact for personal gains, false representation of a material nature that is either misstatement or omission of a material fact, embezzlement, discount of truth, illegal amassing of wealth through dubious means, extortion, act of deception, bribery, theft, false representation and the person receiving the representation has reasonably and understandably relied on it, and host of others and the fact that the receiving party has sustained financial damages from all or any of the above (Albrecht, 2008; Enofe, et.al., 2015; Enofe & Okpako, 2013; Olaoye & Dada, 2017; Udeh & Ugwu, 2018; Zachariah, et al., 2014).

On the basis of different methods used in carrying out fraud, it had been classified into asset misappropriation, corruption and financial misappropriation. The focus of this study is on financial fraud, which is the deviation of an institution's financial resources for satisfaction of selfish desires, using deception techniques, which are identified to include defalcation by way of misappropriation of money or goods or manipulation of accounts (Zachariah, et al., 2014). Crumbley in Osisioma (2012) presented the 3ms of financial reporting fraud which includes: manipulation, falsification or alteration of accounting records or supporting documents from which financial statements are prepared; misrepresentation in or intentional omission from the financial statements of events, transactions, or other significant information; and intentional misapplication of accounting principles relating to amounts, classification, manner of presentation, or disclosure. From the foregoing, this study's scope only borders on financial fraud, which is defined as misrepresentation of a material fact, made intentionally with the intent to deceive so as to gain undue financial resources' from established public institution.

To properly manage the alarming rate of fraud in a certain institution, Almajir and Usaini (2020) point out the need to set up and implement effective and efficient control system that could adequately monitor the daily activities of the institution without leaving any gap for fraudulent activity. Thus, the need for adoption of e-payment system in public institutions to enable people pays bills such as taxes and transfer funds without using cash. On this premise, it is therefore anticipated that e-payment system would significantly reduce the rate of fraud and thereby promote the ability of government institutions to generate more revenue, as it would encourage tax inclusion for larger proportion of the society. However, this could only be possible where the e-payments system is perceived safe and secure by the users.

1.2.3 Dimensions of Perceived Security of E-Payment System and Hypotheses Formulation

Romdhane (2005) reviewed the existing literature and stated that a secure e-payment system must exhibit certain elements, which include confidentiality, authentication,

fraud's prevention, transferability, payment privacy, divisibility, duplicate spending prevention, payer traceability and payment anonymity. However, Hartono, Holsapple, Kim, Na, and Simpson (2014) denoted that the researchers have shown inconsistencies "between the conceptualization of security and the operationalization of the measures of perceived security in empirical studies" (Antinoja & Scherling, 2019). Additionally, the dimensions of confidentiality, recognition and reputation, integrity, availability, and non-repudiation have been acknowledged to be important to the concept of perceived security, although studies tend to capture only one or few of the dimensions at the time (Antinoja & Scherling, 2019). This study operationalized perceived security using four constructs including social recognition and reputation, level of risk-security, level of confidentiality, and perceived trust in the system (Hassan, et al., 2020; Antinoja & Scherling, 2019; Barkhordari et al., 2017; Hartono, et al., 2014).

i Social Recognition and Reputation of the Company Providing the E-Service

The size and reputation of the e-payment system and the e-payment provider (in this case, the KWIRS) played a key role in the perception of security as well as the social factor that most users are familiarized with in respect to using e-payment system, which increases the social acceptance (Antinoja & Scherling, 2019; Bauman & Bachmann, 2017). It has been established that a big well-known company could be more

trustworthy and that social influences increase trust for certain payment providers (Aziza, 2019). This is in congruent with the claim of Järvenpää et al. (2000) that reputation and the size of the merchant are significant to perceived security by the e-payment users. Thus, first hypothesis:

H_01: Social recognition and reputation of the company providing the e-service as a construct of security of the e-payment system does not significantly influence incidence of fraud in Kwara State Internal Revenue Service (KWIRS).

ii. Perceived Level of Risk-Security in E-payment System

Perceived risk as a determinant of system security refers to the extent to which users perceived that a system's portal posed minimal risk, particularly, financial risk in the course of transactions (Sanghita & Indrajit, 2014). Invariably, since security breaches were seen as a threat, the level of associated risks involved in using e-payment system significantly affects users' perception of online security and significantly determines level of user's acceptability of the system (Antinoja & Scherling 2019). Thus, it becomes essential for e-payment provider or merchant (in this case the KWIRS) to provide lucid information on what happens to users' data, in terms of usage and storage, which could help customers to feel more secure about filling in their personal information on the e-payment portals, and to also know how the risk is distributed. Therefore, perceived level of risk is an essential factor that must be

considered as element of system security (Wong & Mo, 2019). Thus, second hypothesis:

$H_0$2: Perceived level of risk-security in e-payment system has no significant effect on incidence of fraud in Kwara State Internal Revenue Service (KWIRS).

iii. Perceived Level of Confidentiality

Confidentiality involves the data being seen by authorized individuals then authentication allows a certain operation to be carried out only after identification, or if there are guarantees of the identity of the party one is dealing with (Aziza, 2019). According to Marlien (2010), perceived security of the system is an essential factor affecting the adoption and operation of e-payment system such as buyer and seller data being kept confidential while being transmitted electronically. Hence, it has been affirmed that the transactions on e-payment systems operation should be confidential, which reassure the customers of privacy-safety (Hartini, et.al, 2020). Since e-payment system of transaction is frail for intrusion, organizations using it are expected to provide extensive privacy and anonymity (Raja & Velmurgan, 2008). This facilitates ease of use of e-payment platform and ensures that customers have more trust in the system for safe transactions. Perceived level of confidentiality is considered a vital factor in enhancing system security (Aziza, 2019; Wong & Mo, 2019). Thus, the third hypothesis:

$H_0$3: Perceived level of confidentiality as a construct of security of the e-payment system has no significant effect on incidence of fraud in Kwara State Internal Revenue Service (KWIRS).

iv. Perceived Level Trust in the System

Generally, trust refers to a form of confidence in platform acting as a partner and in its reliability and integrity (Liao, Liu, & Chen, 2011; Maqableh, Masa'deh, Shannak & Nahar, 2015); Oney, et al., 2017). Aziza (2019) avers that with the increasing adoption of online services, e-payment has become more trustworthy. This comes along with the expansion of the range of suppliers and the size of their delivery networks (Li, Mirosa, & Bremer, 2020).

Online payments have no human interaction, it is based on a computer system but it still incorporates characteristics of trust that can be found in human interactions (Aziza, 2019). Sullivan and Kim (2018) note that users' intention to rely on using an e-payment system may increase by increasing trust through low perceived risk that the users have on the system. Artha (2011) opined that trust is a vital factor in promoting online transactions. Trust is the belief of particular party to others in conducting transaction relationships based on a belief that the person they trust will fulfill all their obligations appropriately and in accordance with expectations (Aziza, 2019).

According to Kim, Kim and Park (2017), perceived trust has a crucial role in predicting user's intention by reducing perceived risk during the transaction. Reichheld and Schefter

(2000) asserted that trust is essential in transactional relationships, particularly those involving high risk such as online transactions. Trust is perceived to be crucial for the success of e-payment system (Zhang, Luximon & Song, 2019; Oney, et al., 2017). Invariably, perceived level of trust towards an e-payment system is a fundamental factor in increasing system security (Wong & Mo, 2019). Thus, the fourth hypothesis:

H₀4: Perceived level of trust as a construct of security of the e-payment system has no significant influence on incidence of fraud in Kwara State Internal Revenue Service (KWIRS).

1.2.4 Theoretical Framework

Theoretical literatures that explain e-payment system depict that there are several extant theories and different approaches that help explain the understanding of the concept. However, theory of innovation translation (TIT) provides suitable theoretical background for the study.

Theory of Innovation Translation

The theory of innovation translation was propounded in 1990 by Arthur Tatnall and it represents an alternative view of the theory of innovation diffusion; which propounded that instead of using an innovation in the form in which it is designed and agreed upon, every potential adopter can translate it into a form that suits their needs. In other words, the potential users of the innovation could decide to modify the innovation in a way that best fits its current system instead of adopting the innovation in the exact way in which

it was proposed. Relating this to this study implies that the innovation here is e-payment system, while the adopter is KWIRS. It is therefore expected that KWIRS adopts e-tax payment system in Nigeria, not in the way it was adopted in other institutions, states, or in other part of the world, rather it should be modified in such a way that best suits both the economic and technological development in the state, so as to definitely reflect appropriate security of the system in which customers can trust.

1.2.5 Empirical Framework

There are a number of studies that discussed e-payment system and organization outcomes.

The study of Yang, et al (2021) examine effect of perceived usefulness, perceived ease of use, social influence, facilitating condition, lifestyle compatibility, and perceived trust on both the intention to use an e-wallet and the adoption of an e-wallet among adults by using the unified theory of acceptance and use of technology (UTAUT). The study employed cross-sectional research design to collect data from 501 respondents using a Google Form. The data were analyzed using partial least square structural equation modelling (PLS-SEM). The results shown that perceived usefulness, perceived ease of use, social influence, lifestyle compatibility, and perceived trust displayed a significant positive effect on both intentions to use an e-wallet and adoption of an e-wallet. The study concluded that managers and policy makers should continuously devise effective

strategies that capture consumers' intention to use and experience of using an e-wallet in the midst of a turbulent market.

Zhang, et al., (2019) determine the role of consumers' perceived security, perceived control, interface design features, and conscientiousness in continuous use of mobile payment services. Primary data was collected from 252 participants using questionnaire, and the data were analysed with structural equation modeling. Findings posit that the perception of interface design features was influenced by conscientiousness. Perceived security was found to be affected by perceived control, the perception of interface design features, and conscientiousness. Moreover, perceived security was identified to have a strong impact on continuous intention to use mobile payment.

Antinoja and Scherling (2019) sought to understand how Swedish millennial consumers' perceptions of online security and online trust of e-payment methods influence online purchasing cancellation. The study was carried out in a qualitative manner by conducting a series of semi-structured face-to-face interviews. 15 Swedish millennials (respondents) were interviewed to collect primary data, which were analyzed using descriptive analysis. The study found that both online trust and online security are perceived as significant determinants when evaluating whether or not the e-payment method could be used.

Aziza (2019) examined the influence of perceived usefulness, ease of use,

behavioral control, security and trust to students on accounting in Universitas Brawijaya towards behavioral intention to use GoPay on GOJEK application. Quantitative approach was used, hence, survey method was employed. The population was all accounting undergraduate students in the Faculty of Economics and Business, Universitas Brawijaya who were active in the period of 2018/2019 with total 1186 students. Outer and inner model with Partial Least Square (PLS) application were used to test the hypotheses. Findings indicate that perceived usefulness, perceives behavioral control, perceived security and perceived level of trust have significant influence on behavioral intention to use GoPay, while perceived ease of use was found to be insignificant in influencing consumers in using GoPay features.

Oney, et al (2017) developed a conceptual model to examine the determinants of perceived security and trust as well as the impact of perceived security and trust on the use of e-payment system (EPS). A randomly selected sample of 299 respondents were analysed through structural equation modelling (SEM). Findings indicate that both perceived security and trust have a significant influence on EPS use. More so, technical protection and past experience were found to be the common determinants of perceived security and trust.

The empirical literature reviewed showed that although many of the findings showed a connection between e-payment system adoption and organizational outcomes, there

were however, variances in their findings and these raise the question of universality of those findings and also if the results could be applied to public establishments within the Nigerian business environment. Additionally, in cases where previous studies revealed positive or significant effect of adoption of e-payment system on organizational performance, none have been conducted to determine the significance of the constructs of perceived security as a major determinant of adoption of e-payment, and subsequently in influencing incidence of fraud, which is the target of this study. Thus, establishing the empirical evidence on the connection underpinning security of e-payment system and incidence of fraud is therefore a timely intervention for policy makers, not only in Kwara State but in the entire country. The variables used in the study were conceptualized to reflect the operational relationship between the study's dependent and independent constructs using input-process-output parameters as shown in figure 1.

2. METHODS

Survey research design was considered appropriate for the study in determining and measuring the respondents' opinions and attitudes towards variables related to perceived security e-payment system and incidence of fraud. The two constructs underlining the study were qualitative in nature, hence, the adoption of survey method.

The population of the study consisted of all the employees of Kwara State Internal Revenue Service (KW-IRS). The total number equals 996 employees working in the headquarter (Ilorin) and across the 16 Local Government Areas of the state (Department of Research and Data Gathering, KW-IRS, 2020). This comprises of 954 staff, 37 management staff and 5 top management staff.

The sample size was determined using Taro Yamane (1967) sample size determination formula as displayed below:

$$n = \frac{N}{1 + N(e^2)}$$

Where;

n= the sample size

N= the population size

e= the acceptable error term

95% confidence level and p=0.5 are assumed

$$n = \frac{996}{1 + 996(0.05^2)}$$

$$n = \frac{996}{1 + 996(0.0025)}$$

$$n = \frac{996}{1 + 2.49}$$

$$n = \frac{996}{3.49}$$

n = 285.38

n = 285

Therefore, the sample size was 285 respondents.

Simple random sampling technique was employed for the selection of the respondents. This gave each of the

respective staff equal chance of being selected in the study.

The collection of primary data was done with the use of questionnaire. The questionnaire was structured into two main parts. The first part focused on the demographic characteristics of the respondents, while the second on questions related to constructs of security of e-payment system and incidence of fraud. These were formulated to provide guidance for proper attainment of the study specific objectives. Likert rating scale of five points was employed, which enabled the respondents to give their opinions to all items based on the scale ranging from strongly agreed (5 point) to strongly disagree (1 point).

The research instrument was subjected to both face and content validity done by at least three experts who are senior lecturers in the Department of Business Administration, University of Ilorin. Cronbach's alpha coefficient was used to analyze the reliability of the study. As depicted in table 1, the Cronbach's alpha (α) value result was 0.839 which signifies s sound reliability of study's instrument in carrying out the analysis.

The data were analysed using multiple regression analysis was used to test the hypotheses formulated for the study.

Hypothetical Model Specification

$IncFru = \beta_0 + \beta_1 SoRecRep_i + \beta_2 PerRiSe_i + \beta_3 PerCon_i + \beta_4 PerTru + \varepsilon$
Where:

IncFru= Incidence of Fraud (Dependent variable)

SoRecRep=Social Recognition and Reputation of the Company (Independent variable)

PerRiSe=Perceived Level of Risk-Security (Independent variable)

PerConf =Perceived Level of Confidentiality (Independent variable)

PerTru=Perceived Level of Trust (Independent variable)

β_0= Intercept of the model.

B_1= Estimate of the parameter of the independent variable in the model.

ε= Error term.

3. RESULTS

The responses to questionnaires administered (table 2) depicts that 261 out of 285 copies of the questionnaire representing 91.6% were returned and considered suitable for the study. This connotes that majority of the respondents positively responded to the questionnaire.

The demographic data's analysis of respondents as displayed in table 3 illustrates that majority were males with 63.6%, females constitute 36.4% of the total respondents. The age distribution depicts that 17.6% were between 20-29 years; 43.7% were within the age range of 30-39 years; 32.5% were within 40-49 years; and 6.1% were 50-59 years. This implies that majority of the staff of the establishment is typically younger adults, who could appropriately understand the concepts under discourse. Marital status of the respondents revealed that 36.0% were singles; 62.8% which constitute the majority were married; and 1.1% of

the respondents were widowed. Educational qualification of the respondents revealed that 8.8% had NCE/OND; 73.9% had H.N.D/B.Sc./ or its equivalent; 16.9% had Masters or its equivalent; and 0.4% had Ph.D. This implies that a larger proportion of the respondents are well educated and could appropriately understand the concept of security of e-payment system and how its dimensions affect institutional performance. Distribution of the respondents by years of experience revealed that 15.3% had between 1-2 years' experience; 56.3% had between 3-4 years; and 28.4% had between 5-6yrs. Since KW-IRS as a government establishment was officially founded in 2015, it implies that majority of the respondents have considerable number of work experience with the establishment which would helped them understand the operational phenomenon of the establishment, thereby boosting their experience in contributing significantly to study.

As demonstrated in table 4-6, multiple regression analysis was used to test whether or not perceived security of e-payment significantly influence incidence of fraud in KW-IRS. The model summary as shown in table 4 reveals that the dimensions of perceived security of e-payment system are positive and significant predictors of incidence of fraud (IncFru). The multiple correlation coefficient (R) value of 0.781 (78.1%) signifies that there is significant relationship between incidence of fraud (IncFru) and perceived security of payment method, depicted by constructs of social recognition and reputation of the company (SoRecRep); perceived level of risk-security (PerRiSe); perceived level of confidentiality (PerConf); and perceived level of trust (PerTru).

The R-square value of 0.609 (60.9%) indicates that the independent variables of social recognition and reputation of the company (SoRecRep); perceived level of risk-security (PerRiSe); perceived level of confidentiality (PerConf); and perceived level of trust (PerTru) have a combine effect of 0.609 (60.9%) on the dependent variable of incidence of fraud (IncFru).

The adjusted R^2 value of 0.603 (60.3%) depicts that social recognition and reputation of the company (SoRecRep); perceived level of risk-security (PerRiSe); perceived level of confidentiality (PerConf); and perceived level of trust (PerTru) as independent variables actually contribute to variation in the level of incidence of fraud (IncFru) in KW-IRS. This is good enough in determining the goodness of fit for the model, hence, the regression model proved to be very useful for making predictions.

Table 5 described the overall diagnostic test of significant using Analysis of Variance (ANOVA) between constructs of perceived security of e-payment method and incidence of fraud. The ANOVA results indicate that the significant value of the F-statistics is $F=99.859>F\text{-table}=4.29$ at a degree of freedom of $(4, 256)$ with p-value=0.00 which is less than 0.05 or 5% error term. This posits that the model of the study is well fitted.

Therefore, it is well established that perceived security of e-payment method is essential in influencing incidence of fraud in KW-IRS.

As portrayed in table 6, the estimated equation of the model could be expressed as $IncFru = \beta 0 + \beta_1 SoRecRep_i + \beta_2 PerRiSe_i + \beta_3 PerConf_i + \beta_4 PerTru + \varepsilon$.

Table 6 equally described that incidence of fraud (IncFru) would be equal to 3.977 when all other variables remained constant. It would be however significantly influenced by 0.120, 0.193, 0.396, and 0.525 respectively when there is a unit increase in social recognition and reputation of the company (SoRecRep]; perceived level of risk-security (PerRiSe); perceived level of confidentiality (PerConf); perceived level of trust (PerTru) respectively, while other variables remain constant.

Additionally, the table depicted that the standardized beta coefficient in respect to social recognition and reputation of the company (SoRecRep) was 0.249 with t-test value of 4.091 at 5% level of significance. This points out that the variable as a construct of perceived security is a positive predictor of incidence of fraud (IncFru) in KW-IRS. The standardized beta coefficient in respect to perceived level of risk-security (PerRiSe) was 0.346 with t-test value of 5.912 at 5% level of significance. This implies that the variable as a construct of security of e-payment system is significantly relevant in predicting incidence of fraud (IncFru) in KW-IRS.

The standardized beta coefficient in respect to perceived level of confidentiality (PerConf) was depicted to be 0.910 with t-test value of 7.767 at 5% level of significance. This indicates that the variable as a construct of perceived security could positively influence incidence of fraud (IncFru) in KW-IRS.

The standardized beta coefficient of perceived level of trust (PerTru) was 1.132, with t-test value of 12.665 at 5% significant level. This signifies that the variable as a construct of perceived security is statistically significant to predict incidence of fraud (IncFru) in KW-IRS.

The summary of the regression analysis results as shown in table 7, therefore, depicts that since the calculated p-value is less than the critical/tabulated p-value of 0.05, and that all the constructs of security of e-payment system positively predict incidence of fraud in KW-IRS, the null hypotheses were therefore rejected which gives room for the adoption of alternative hypotheses, thus, establishing the fact that perceived security of e-payment system has significant effect on incidence of fraud in KW-IRS.

4. DISCUSSION

This study examined perceived security of e-payment system and its relative effect on incidence of fraud, with particular reference to Kwara State Internal Revenue Service (KW-IRS), Nigeria. Security of e-payment system was sited to stand as the explorative variable and incidence of fraud as dependent variable, while the

degree of influence was determined by testing four hypotheses formulated in line with the study specific objectives, so as to arrive at conclusive findings. The connotation of the demographic characteristics of the respondents is that they cut across diverse age categories, gender, marital and have various years of experience, which helped the study gain assorted opinions on issues relating to perceived security of e-payment system and how its dimensions affect incidence of fraud.

Findings from hypotheses testing revealed that the four constructs of security of e-payment system hypothesized in the study's model are positive and significant predictors of incidence of fraud in KW-IRS. This posits that the management of Kwara State internal revenue (KW-IRS) service should concentrate more effort and resources on enhancing the security aspects of utilizing e-payment systems in order to further influence reduction in incidence of fraud and thereby promoting operational efficiency as a key performance parameter of the establishment (Aziza, 2019). The finding is in agreement with previous studies such as Antinoja and Scherling (2019); Aziza (2019); Kim et al, (2017); Oney, et al (2017); Wong and Mo (2019); Yang, et al (2021); Zhang, et al., (2019), which established that dimensions of security of e-payment system significantly influence perceived usefulness of the system, which invariably affect e-payment adoption. Thus, perceived security of e-payment system among users (in this case the tax payers in Kwara State, Nigeria) significantly influences perceived usefulness of the system and then behavioral intent to use e-payment system among tax payers in Kwara State, which will further influence reduction in incidence of fraud.

The analysis further reveals that among the four enabling factors of security of e-payment system, perceived level of trust (PerTru) with the standardized beta coefficient of 1.132 and t-test value of 12.665 at 5% significant level contributed the most as a construct of perceived security in influencing changes in the level of incidence of fraud (IncFru). It was followed by perceived level of confidentiality (PerConf), then by perceived level of risk-security (PerRiSe), and lastly by social recognition and reputation of the company (SoRecRep), which was found to contribute the least.

Therefore, perceived level of trust (PerTru) dimension of security of e-payment system is more significantly important to users of KW-IRS' e-payment system than other three dimensions, which portrayed that users usually desire payment system that confirmed the element of trust as a crucial parameter in predicting users' intention to use the system and this promote a sense of confidence towards the payment process.

5. CONCLUSION AND RECOMMENDATIONS

Drawing implications from the findings, this study concludes that perceived security of e-payment system is a viable tool that can be essentially use in significantly influencing reduction in incidence of

fraud in public establishments, with particular reference to Kwara State Internal Revenue (KW-IRS) Nigeria. The implication of the foregoing is that proper implementation of e-payment systems in government establishments would help to fast track implementation of government policies of higher revenue generation and lower incidence of process in the system processes. This is made possible by eliminating delays in payment process and by making transaction medium more transparent, thereby ensuring proper accountability of the system. This will further reduce incidence of fraud and corruption by minimizing interaction of government officials with tax payers and promote accountability in order to ensure that public resources are directed towards the attainment of targeted objectives. A sound security system of e-payment would equally help to achieve effective and efficient government financial performance system, thereby facilitating enhancement of real-time reporting system and ensuring transparent financial reporting process in the public sector.

The following specific recommendations were made:

E-payment system in Nigeria has shown tremendous growth, but there are still a lot to be done to increase its usage. As extant literature shown that a larger proportion of transactions in Nigeria is still been done using cash basis, particularly in the public sector. Thus, it is requiring that more efforts are made by the government to widen the level of coverage of e-payment system in the country. These demands for high level of innovation, proper affiliation with private sector in expending the existing internet facilities, and establishing a better legal framework so as to enhance the ease of use and safety of the users.

Additionally, since it was established that perceived trust contributed most as a construct of perceived security, which is invariably significant to reduction in incidence of fraud, it is therefore essential for government and its agencies to partner with technocrats and financial institutions to organize free seminars and workshops, particularly for rural area's people, in order to further enlighten less educated people in respect to uses of e-payment system, and also give necessary information regarding security and privacy of their account.
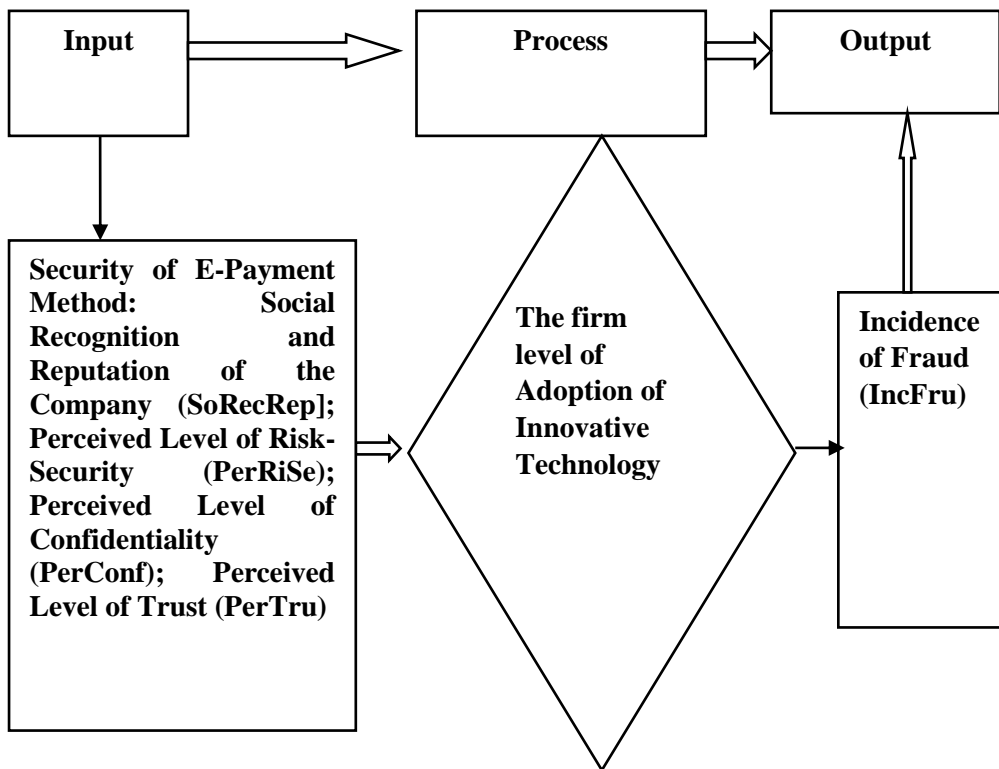
APPENDIX

```
┌──────────┐        ┌──────────┐      ┌──────────┐
│  Input   │═══════▶│ Process  │═════▶│  Output  │
└──────────┘        └──────────┘      └──────────┘
```

Security of E-Payment Method: Social Recognition and Reputation of the Company (SoRecRep]; Perceived Level of Risk-Security (PerRiSe); Perceived Level of Confidentiality (PerConf); Perceived Level of Trust (PerTru)

The firm level of Adoption of Innovative Technology

Incidence of Fraud (IncFru)

Figure 1: Study Conceptualization

Source: Author's Design (2022)

Table 1: Cronbach's Alpha Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha based on standardized items	Number of items
0.839	0.839	20

Source: SPSS Printout, 2022

Table 2: Analysis of Responses to Questionnaire (Customers/tax payers)

Description	Frequency	Percentage
Administered	285	100.0
Returned	261	91.6
Not Returned	024	08.4

Source: Field Survey, 2022

Table 3: Analysis of Respondents Demographic Data

Demographic Characteristic	Frequency	Percentage
Gender: Male	166	63.6
Female	95	36.4
Total	261	100.0
AGE: 20-29yrs	46	17.6
30-39yrs	114	43.7
40-49yrs	85	32.5
50-59yrs	16	6.1
Total	261	100.0
Marital Status: Single	94	36.0
Married	164	62.8
Widowed	3	1.1
Total	261	100.0
Highest Educational Qualification: N.C.E/OND	23	8.8
H.N.D/ B.Sc.	193	73.9
M.Sc/MBA or Equivalent	44	16.9
Ph.D	1	.4
Total	261	100.0
Years of experience		
1-2yrs	40	15.3
3-4yrs	147	56.3
5-6yrs	74	28.4
Total	261	100.0

Source: Field Survey, 2022

Table 4: Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.781[a]	.609	.603	.424

a. Predictors: (Constant), PerTru, PerConf, PerRiSe, SoRecRep

Source: Author's Computation, 2022

Table 5: ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	71.790	4	17.948	99.859	.000[b]
	Residual	46.011	256	.180		
	Total	117.801	260			

a. Dependent Variable: IncFru
b. Predictors: (Constant), PerTru, PerConf, PerRiSe, SoRecRep
Source: Author's Computation, 2022

Table 6: Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	T	Sig.
		B	Std. Error	Beta		
1	(Constant)	3.977	.122		32.636	.000
	SoRecRep	.120	.029	.249	4.091	.001
	PerRiSe	.193	.033	.346	5.912	.000
	PerConf	.396	.051	.910	7.767	.000
	PerTru	.525	.041	1.132	12.665	.000

a. Dependent Variable: IncFru
Source: Author's Computation, 2022

Table 7: Summary of Findings

Hypothesis	Beta Coefficients (β)	T	Sig. value	Remarks
H_01: Social recognition and reputation of the company providing the e-service as a construct of security of the e-payment system does not significantly influence incidence of fraud in Kwara State Internal Revenue Service (KWIRS).	0.120	4.091	.001	Rejected
H_02: Perceived level of risk-security in e-payment system has no significant effect on incidence of fraud in Kwara State Internal Revenue Service (KWIRS).	0.193	5.912	.000	Rejected
H_03: Perceived level of confidentiality as a construct of security of the e-payment system has no significant effect on incidence of fraud in Kwara	0.396	7.767	.000	Rejected

State Internal Revenue Service (KWIRS).				
H₀4: Perceived level of trust as a construct of security of the e-payment system has no significant influence on incidence of fraud in Kwara State Internal Revenue Service (KWIRS).	0.525	12.665	.000	Rejected

Source: Author's Computation, 2022

REFERENCES

Adeyinka, T. (2012). Determinants of E- Payment Systems Success: A User's Satisfaction Perspective. *International Journal of E-Adoption*, 4(3), 15-38. DOI:10.4018/jea.2012070102

Albrecht, W.S. (2008). Current trends in fraud and its detection: A global perspective. *Information Security Journal*, 17, 1-32.

Antinoja, R. & Scherling, D. (2019). *The Effects of E- payment Methods on Online Purchasing Cancellation: An empirical study on Swedish consumers' perception of trust and security in e-payments*. Unpublished Bachelor Thesis of Business Administration, Marketing Management & International Management, Jönköping International Business School, Jönköping University

Artha, U. (2011). *Pengaruh Persepsi Kegunaan, Persepsi Kemudahan, Persepsi Risiko, Kepercayaan, Inovasi Pribadi, dan Kesesuaian Terhadap Sikap Penggunaan E Commerce. Skripsi*. Jurusan Akuntansi Fakultas Ekonomi dan Bisnis Universitas Brawijaya.

Aziza, M.O. (2019). *The influence of perceived usefulness, ease of use, behavioral control, security and trust towards the behavioral intention to use go-pay (A case study on accunting students in Universitas Brawijaya)*. Unpublished thesis of the Universitas Brawijaya Malang.

Balunywa, W., Nangoli, S., Mugerwa, G. W., Teko, J., & Mayoka, K. G. (2014). An analysis of fiscal decentralization as a strategy for improving revenue performance in Ugandan Local governments. *Journal of Research in International Business and Management,* 4 (2), 28-36. doi:http:/dx.doi.org/10.14303/jribm.2013.011

Barkhordari, M., Nourollah, Z., Mashayekhi, H., Mashayekhi, Y., Ahangar, M.S., (2017). Factors influencing adoption of e-payment systems: an empirical study on Iranian customers. *ISEB,* 15(1), 89–116.

Bauman, A., & Bachmann, R. (2017). Online Consumer Trust: Trends

in Research. *Journal of Technology Management & Innovation*, 12(2), 68-79. doi:10.4067/s0718-27242017000200008

Enofe, A. O. Idemudia, N. G. & Emmanuel, G.U. (2015). Forensic Accounting a Panacea to Fraud Reduction in Nigeria Firms. *Journal of Accounting and Financial Management,*1(8), 848-64.

Fang, X., Chan, S., Brzezinski, J., & Xu, S. (2005). Moderating Effects of Task Type on Wireless Technology Acceptance. *Journal of Management Information Systems*, 22(3), 123-157. doi: 10.2753/mis0742- 1222220305

Fianyi, I. (2015). Curbing cybercrime and Enhancing e-commerce security with Digital Forensics. *International Journal of Computer Science Issues,* 12 (6).

Flavián, C., Guinalíu, M., & Gurrea, R. (2006). The role played by perceived usability, satisfaction and consumer trust on website loyalty. *Information & Management*, 43(1), 1-14. doi: 10.1016/j.im.2005.01.002

Gbegi, D. O., & Adebisi, J. F. (2014). Forensic skills and techniques in fraud investigations in the Nigerian public sector. *Mediterranean Journal of Social Sciences,* 5(3), 243-252.

Hartini, A., Tan, Z.Y., & Mohammed, H.B. (2020). The Factors that Affecting Consumer Intention to Utilize the Electronic Payment System in Malaysia. *Journal of Technology Management and Technopreneurship,* 08, 129–138

Hartono, E., Holsapple, C., Kim, K., Na, K., & Simpson, J. (2014). Measuring perceived security in B2C electronic commerce website usage: A respecification and validation. *Decision Support Systems*, 62, 11-21. doi: 10.1016/j.dss.2014.02.006.

Hassan, M.A., Shukur, Z., & Hasan, M.K. (2020). An efficient secure electronic payment system for e-commerce *Computers,* 9 (66); 1-13. doi: 10.3390/computers9030066.

Järvenpää, S.L., Tractinsky, N. & Vitale, M. (2000). Consumer Trust in an Internet Store. *Information Technology and Management*, 1, 45-71. http://dx.doi.org/10.1023/A:1019104520776.

Kim, S.Y., Kim, J.U., & Park, S.C. (2017). The Effects of Perceived Value, Website Trust and Hotel Trust on Online Hotel Booking Intention. *Sustainability*, 9, 22-62.

Kim, C., Tao, W., Shin, N., & Kim, K. S. (2010). An empirical study of customers' perceptions of security and trust in e-payment systems. *Electronic commerce research and applications*, 9(1), 84-95.

Li, C., Mirosa, M., & Bremer, P.J. (2020). Review of Online Food Delivery Platforms and their Impacts on Sustainability. *Sustainability*, 12, 5528.

Liao, C., Liu, C. C., & Chen, K. (2011). Examining the impact of privacy, trust and risk perceptions beyond monetary transactions: An integrated model. *Electronic Commerce Research and Applications*, 10, 702–715.

Maqableh, M., Masa'deh, R.M.T., Shannak, R.O. & Nahar, K.M. (2015). Perceived Trust and Payment Methods: An Empirical Study of MarkaVIP Company. International Journal of Communications, Network and System Sciences, 8 ,409-427. http://dx.doi.org/10.4236/ijcns.2015.811038.

Marlien, R.A.P. (2010). Pengaruh Reputasi, Privasi, dan Keamanan Terhadap Kepercayaan (Trust) Pengguna Internet di Semarang Dalam Sistem E- commerce. *Jurnal Manajemen danBisnis,*14(2).

Masihuddin, M., Islam Khan, B.U., Islam Mattoo, M.M.U., Olanrewaju, R.F. (2017). A Survey on E-Payment Systems: Elements, Adoption, Architecture, Challenges and Security Concepts. *Indian J. Sci. Technol.*, 10, 1–19.

Ngotho, J. & Kerongo, F. (2014). Determinants of in Developing Countries: Kenya's Tax Collection Perspective. *Journal of Management and Business Administration*, 1(1).

Njanja, N.M. (2014). *Strategies adopted by the county government of Mombasa in raising revenue*. Unpublished MBA Research Project, Nairobi: University of Nairobi, Kenya.

Odukoya, O.O, & Samsudin, R.S. (2021). Knowledge capability and fraud risk assessment in Nigeria deposit money banks: The mediating effect of problem representation. *Cogent Business & Management*, 8, (1), 1899450, DOI: 10.1080/23311975.2021.1899450

Ogbeide, S.O. (2018). Empirical assessment of frauds on the financial performance of banking sector in Nigeria. *International Journal of Research Studies in Management*, 7 (1), 75-84.

Olaoye, C.O., & Dada, R.A., (2017). The Roles of Auditors in 0Fraud Detection and Prevention in Nigeria Deposit Money Banks: Evidence from Southwest. *European Scientific Journal*, 13 (31), 290-306. Doi:10.19044/esj.2017.v13n31p290

Oney, E., Guven, G.O., & Rizvi, W.H. (2017). The determinants of electronic payment systems usage from consumers' perspective. *Economic Research*, 30(1), 394-415. DOI:10.1080/1331677X.2017.1305791

Osisioma, B.C. (2012). *Fraud prevention in Nigeria: Applying the forensic accounting tool*. A paper presented at a three-day workshop on the effective accounting officer in the current financial challenges, organised

by Entrepreneurial Centre, University of Port Harcourt, July 13.

Raja, J., & Velmurgan, M. (2008). E-payments: Problems and prospects. *Journal of internet banking and commerce,* 13(1), 1-17.

Reichheld, F. F., & Schefter, P. (2000). E-loyalty. *Harvard Business Review*, 78, 105–113.

Romdhane, C., (2005). Security implications of electronic commerce: a survey of consumers and businesses. *Internet Research: Electronic Networking Applications and Policy*, 9(5), 372–382.

Sanghita, R. & Indrajit, S. (2014). Determinants of Customers' Acceptance of Electronic Payment System in Indian Banking Sector – A Study. *International Journal of Scientific & Engineering Research*, 5(1), 177-187.

Sullivan, Y.W. & Kim, D.J. (2018). Assessing the effects of consumers' product evaluations and trust on repurchase intention in e-commerce environments. *International Journal of Information Management,* 39, 199–219.

Tsiakis, T. & Sthephanides, G. (2005). The Concept of Security

Zhang, J., Luximon, Y., & Song, Y., (2019). The Role of Consumers' Perceived Security, Perceived Control, Interface Design Features, and Conscientiousness

and Trust in Electronic Payments. *Computers and Security*, 24, 10-15.

Udeh, S. N., & Ugwu, J. I. (2018). Fraud in Nigerian Banking Sector. *International Journal of Academic Research in Business and Social Sciences*, 8(5),585–603. DOI: 10.6007/IJARBSS/v8i5/4159

Wong, W.H., & Mo, W.Y., (2019). A Study of Consumer Intention of Mobile Payment in Hong Kong, Based on Perceived Risk, Perceived Trust, Perceived Security and Technological Acceptance Model. *Journal of Advertisement Management Science,* 7, 33–38.

Yang, M., Mamun, A.A., Mohiuddin, M., Nawi, N.C., & Zainol, N.R. (2021). Cashless Transactions: A Study on Intention and Adoption of e-Wallets. *Sustainability,* 13(831), 1-18. https://doi.org/10.3390/su13020831

Zachariah, P., Masoyi, A.D., Ernest, E.I., & Gabriel, A.O. (2014). Application of Forensic Auditing in Reduding Fraud Cases in Nigeria Money Deposit Banks. *Global Journal of Management and Business Research*, 24 (3), 14-22.

in Continuous Use of Mobile Payment Services. *Sustainability*, 11, 6843; 1-16. doi:10.3390/su11236843