Consumer Susceptibility to E-banking Services: Evidence from Retail Banking Sector of The Gambia

Ismaila Bojang and Lamin B. Ceesay

Abstract — Electronic banking (e-banking) is a growing phenomenon in the world of a seamless, dynamic business environment. E-banking allows customers to conduct financial banking transactions through the interface of electronic devices. Thus, the purpose of this research is to investigate consumer behaviour in the adoption of e-banking services among retail banking clients of The Gambia. A survey of 144 retail banking customers participated in the study. Results confirm that perceived security and privacy concerns have a significant impact on perceived trust in the adoption of e-banking services. Our original contribution to the literature is the empirical examination of this new phenomenon (e-banking) among a largely conservative (of whom are adopters of the traditional banking services instead) retail consumers in the Gambia. Results also add that female respondents are more susceptible to e-banking security and privacy concerns. It can be deduced from the findings, that despite the growing adoption of e-banking practices globally, we are seeing a significant consumer susceptibility to e-banking. For example, economies with high internet-based connectivity experience intense use of e-banking services unlike the case of consumers in the third world economies, particularly in The Gambia.

Index terms - E-banking, financial institutions; privacy concern, The Gambia.

I. INTRODUCTION

Over the last few years, electronic commerce has gone through a rapid change [29] and thus, a catalyst in transforming the manner of business transactions and operations all over the world [26]. Several internet-based services influence the nature of the general business landscape: e-commerce, e-health, e-recruitment, and social networking. In the face of dynamism of the banking industry, electronic-based financial transactions are used to address transaction efficiency [24] and customer satisfaction [29].

As a growing phenomenon in the world of a seamless business environment, electronic banking (e-banking) allows customers to conduct financial transactions through the interface of electronic devices [16] Specifically, e-banking is a broad term that leverages an internet-based, online banking service. It also extends to the use of automatic teller machines (ATMs) for withdrawals, deposits and making payments, without having to go online [8]. The complexity involving financial transaction from customer supports and relationship management, exchange rates, and specific economic dynamics increase the popularity of e-banking across the globe. The adoption of e-banking provides market opportunities, quality and efficient service delivery and profitability compared to the traditional banking services (e.g. 13; 25).

Most financial institutions have autonomous e-banking structure (an e-banking window) that complements the traditional branch networks. This practice thus serves as an alternative channel to secure the loyalty of regular customers, reduce operating costs and increase transaction efficiency. The e-banking via telephones and online banking intensify the industry competition and foster greater satisfaction and stronger ties with clients [13]. For the customer, e-banking enhances their convenience of remote, distance financial transactions. According to Liebana-Cabanillas, et al., [21] e-banking does not only facilitate financial transactions, but it also enables synergies between trading partners (even distant ones), and quality customer engagement and satisfaction. The customer depends on online information from company websites and the convenience of transacting business online or via other digital platforms. E-banking is the use of a computer to retrieve and process banking data (statements, transactions details, etc.) and to initiate transactions (payments, transfers, requests for services, etc.) directly with a bank or other financial services provider remotely via a telecommunications network [25]. Scholars argue that tighter deregulation of the financial sector and intense competition in the industry and proliferation of internet use has intensified the spread of e-banking systems. The traditional banking services conducted via bank branches have, to a greater extend loss its prominence in the industry.

Rashad and colleagues suggest that a significant number of customers refused to engage in online transactions for fear of disclosure of private information [29]. The result of which may deter customer selection of e-banking services. However, it is not clear whether customer susceptibility affects their adoption of internet banking services [e.g. 38]. Unless the banks assure client online security, these fears may continue to limit the potentials of e-banking in developing economies like The Gambia. Therefore, this research aims to investigate how consumer susceptibility to e-banking affect their trust in the adoption of e-banking services.

While there is an increasing global proliferation of e-banking, unfortunately, banks in The Gambia offers only a limited range of e-banking services to their customers. Some of these services include Mobile top-ups, online bill payments, money transfer services, online financial tracking services, and ATMs. This could be as a result of customer low adoption of e-banking services. The banking sector comprises of a mix of local (Gambian-based) banks, Nigerians banks and few other Regional and International banks. A cross-section of retail banking clients comprises the primary sources of the empirical data. The individual retail consumers make up to 40% of the population [5]. These categories of the populations are mainly civil servants.

Published on April 16, 2020.

Authors: Lamin B. Ceesay, University of The Gambia, School of Business and Public Administration, The Gambia.
(e-mail: bcceesay@utg.edu.gm)
Ismaila Bojang, University of the Gambia, School of Business and Public Administration, the Gambia.
(e-mail: bogissbo@gmail.com)

DOI: http://dx.doi.org/10.24018/ejbmr.2020.5.2.286
and employees from the private sector. Thus, the level of earnings among these groups is a predictor of their behavioral adoption of e-banking, due to the transaction charges associated with these services. We use an online survey of retail banking clients to elicit perceptions of the adoption of e-banking services.

Based on the review of relevant literature, key determinants affecting the adoption of e-banking services have been identified and constituted the research model. These factors include perceived risk, perceived security, privacy concerns and consumer trust. We use multiple linear regression to evaluate consumer perception of these measures. The first section of the study is a theoretical background and hypothesis development. This section examines the theory of e-commerce and e-banking operations. The second section illustrates the research design and method of the study. The third section discusses the research findings which are followed by the discussions of the findings and recommendations for future research agenda and practice.

II. PRIOR LITERATURE AND HYPOTHESES

A. The theory of e-banking

E-commerce entails business communications and transactions over online networks. Through these digital communications platforms, purchase of goods/services and exchanges of financial services are efficient and timely. E-commerce or e-businesses are new phenomena that are drastically changing the business landscape that are quite distinct from the traditional brick and mortar interfaces.

E-banking is a distinct form of e-commerce that leverages the internet-based and digital platforms to conduct financial transactions. Banking industry relies on these new communication mechanisms to enhance value-added services and offers customer convenience [25]. FinCen (2000) describes the practice of e-banking as an inclusive term, enabling virtual financial transactions without going to physical bank branches. Through virtual telecommunications network systems, e-banking processes banking data (statements, transaction details, etc.) and initiate transactions (payments, transfers, requests for services, etc.) directly with a bank or other financial institutions. Today, such services form an integral function of several financial institutions, Yousaafzai et al., [38] argued that the survival of internet banking is dependent on the bank’s capability to assure customers to engage in online banking. Thus, internet-based customer relationship is a critical aspect of building online customers [13].

Studies [e.g. 16] suggests that the evolution of internet banking brought about great improvements in banking, changing customer banking behavior and enabling financial transaction through integrated electronic media. Internet banking allows bank’s customers to place requests of financial information and conduct retail banking operation through interfaces of computers, television or mobile phones [11; 35]. This thus leads to the increased attention of managers of financial institutions towards consumer behavioral aspects to e-banking [37]. This move by banks reflects the dynamic nature of consumer behaviour as it can change over time recognizing the dynamic, and ever-changing technology-based business landscape.

B. Hypothesis development

Studies on e-banking observe different dimensions of consumer behaviour research, for instance, customer loyalty and word of mouth (WOM) [9], satisfaction and trust [21], customer perceived power, risk and privacy in digital information [3] service quality, satisfaction, trust and loyalty [8], privacy concerns [34], etc. One specific tool or mechanism that online banks commonly use to manage customer perceptions of their security is the security policy [24].

The security policy is usually a clear statement on the bank’s website, indicating measures or steps taken to protect the information supplied by their customers. These measures may be in the form of encryption, firewalls, server authentication as well as password protection [23]. According to Yousaafzai et al. [37], recognizing critical aspects of online security help to reassure customers about the security of their transactions and thus creating confidence. Hoffman et al. stated that 63% of online end-users deliberately delay in providing their data as a result of the lack of confidence in online sites. To mitigate the potential vulnerabilities regarding security, several vendors have developed various solutions in both software and hardware-based solutions. Individuals have different perceptions regarding the security of personal information [22]. Therefore, consumer security concerns surrounding e-banking may affect their adoption of banking services conducted via online platforms.

Customer’s conceptualization of risk (in terms of uncertainty and consequences) associated with e-banking maybe critical in consumer banking decision [10]. The current focus of risk to information disclosure is at the level of “layer protocols” and the shortcomings in end-to-end computing [25]. However, businesses are faced with challenges of low-risk solutions to reduce the level of perceived risk associated with online banking. Unless the banks assure clients about risks of online banking, these fears may continue to limit the potentials of e-banking. Investments in risky online capabilities to assure consumer confidence is critical to conducting online banking and thus customer confidence. E-business is intricately linked with consumer privacy concerns. Privacy may include consumers concerns over the collection and subsequent access, use and disclosure of their private and personal information. Consumer evaluations as well as their decisions to purchase online rely on their assessment of privacy concerns [e.g. 14; 15; 19]. Further, Chellapa [6] argued that customers may still have subjected beliefs regarding how the information they shared is used.

The proliferation of e-banking may invoke consumer online trust. The question: can e-banking services be relied upon? This thus remain a salient issue confronting financial institutions engaged in e-banking business. The e-commerce environment is perceived to be risky and impersonal [27] and thus an important subject of discussion in e-banking spheres. Research hypotheses as are follows:

H1. High perceived security concerns affect customer trust in the adoption of e-banking services.

H2. High perceived risks affect customer trust in the adoption of e-banking services.

H3. High perceived privacy concerns affect customer trust in the adoption of e-banking services.
III. STUDY METHODS

A. Sampling

Using a primary data collection method was employed through an online survey to collect empirical data from selected retail banking clients of The Gambia. A convenient sampling of respondents was carried out. An online survey questionnaire was administered to collect relevant data on respondents. All respondents were invited to participate in this study through one of the most used social media such as Facebook while the few others were reached through email. The questionnaire is divided into two parts, namely, the first part is the bio information on respondents such as their age range, gender, level of education attained, usage of online banking and their impression. The objective of these questions is to capture the specific profile of respondents for practical managerial implications (such as customer targeting, sales promotion, communication, etc.) and a sphere for future research agenda. The second part of the questionnaire touches on the evaluation of consumer perception of relevant online-banking factors. These factors gauge consumer opinion according to the five-point Likert scale (ranging from strongly disagree to strongly agree). According to Saunders et al., [32] this method of questioning allows respondents to elicit behavioral motivation accordingly.

B. Defining Measurement Scales and Reliability

Following several authors [e.g. 37; 4, etc.], measurement scales were adopted and used in this study. These scales evaluate consumer online banking perception in terms of perceived transaction risk, perceived security, perceived privacy, and perceived trust. All these constructs are measures according to five-point Likert’s scale ranging from one (1) very unlikely, two (2) unlikely, three (3) undecided/neutral, four (4) likely, and five (5) very likely. A total of 16 statements adopted from several pieces of literature, constitute the main scale items used in this study.

Perceived risk of Cox, Cox, and Zimet [10] was adopted as cited in Bruner II [2, p. 306-307], used to measure customer’s conceptualization of risk (in terms of uncertainty and consequences), is used to evaluate risks associated with e-banking, according to customers’ perspectives. The original studies [10] reported to have alphas of 0.81, thus confirms the suitability of this construct. Five (5) Scale items were used to evaluate the perceived risk associated with transaction risks, financial loss, personal information loss and bank account information. The measurement scale perceived risk with a reliability value was found to be far less than the acceptable level of confidence (0.60). Through SPSS output, excluding a single statement that seems to have dominated the largest percentage of the Cronbach’s alpha value was eliminated and the new value (0.737) is accepted in this study. The statistical mean (m= 8.84) and standard deviation (2.99) of the scale were given using the four statements, instead of the original five. The result shows that the scale, thus, has met internal validity and reliability.

Perceived security [31] as cited in Bruner II, [2, p. 320] was adopted. This scales measures consumer’s perception of personal and financial security associated with a given transaction, adopted here as e-banking services. The authors reported alpha 0.76, thus a reliable measure for this study. Revised and adopted, the study uses five (5) statements that evaluate consumer perception of a bank’s security system, confirmation of identities, unauthorized access, unauthorized changes and secure environment. The scale perceived security has reliability with a high confidence level (0.905) with a statistical mean (m=18.57) and standard deviation (5.08). The scale thus guarantees a high degree of reliability maintained in the current study.

Perceived privacy scales [34] was adopted. The authors recognized five core principles of privacy concerns that guide the development of online business, and thus consumers evaluation of these issues is the central focus of this study. The perceived privacy scale has a Cronbach’s alpha (0.84), mean (m=15.47) and standard deviation (5.22) confirms the confidence level of this scale. Perceived trust in the brand by [33] was adopted and used to measure consumer’s perception of electronic banking as “reliable and worthy of trust” [cited in [2, p. 373]. The original studies reported composite reliability of the scales ranging from 0.77 and 0.89 in study one and two respectively [33]. The perceived trust scale has a Cronbach’s alpha (0.773), mean (m=9.56) and standard deviation (3.09) confirmed the satisfactory level of internal confidence in this scale.

Malhotra et al., [22] argued that a reliability test is used to determine the stability and consistency with which the research instruments measure the constructs. Scholars further suggested that the coefficient varies from 0-1 and a value of 0.6 or less generally implies unsatisfactory internal consistency [22]. A table below is a descriptive statistic of the measurement scales in the current study.

### TABLE 1: MEANS, STANDARD DEVIATION AND CRONBACH’S ALPHA

<table>
<thead>
<tr>
<th>Constructs</th>
<th>Number of statements</th>
<th>Mean</th>
<th>Standard deviation</th>
<th>Original Cronbach’s Alpha value</th>
<th>New Cronbach’s Alpha value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Perceived risk</td>
<td>3</td>
<td>8.84</td>
<td>2.99</td>
<td>0.816</td>
<td>0.737</td>
</tr>
<tr>
<td>Perceived security</td>
<td>5</td>
<td>18.57</td>
<td>5.08</td>
<td>0.763</td>
<td>0.905</td>
</tr>
<tr>
<td>Perceived privacy</td>
<td>5</td>
<td>15.47</td>
<td>2.22</td>
<td>0.760</td>
<td>0.846</td>
</tr>
<tr>
<td>Perceived trust</td>
<td>3</td>
<td>9.56</td>
<td>3.09</td>
<td>0.771</td>
<td>0.773</td>
</tr>
</tbody>
</table>

IV. RESULTS

A. Description of sample population and sampling

The research adopts a quantitative through online questionnaire. The questionnaires were distributed to the target respondents in the Gambia through electronic means which includes emails and social media platforms, mainly through Facebook and email addresses. The reason for using these means is to save cost as well as increase the chances of getting full responses. The population size targeted was a
total of three hundred (no=300) participants out of which a random sample of two hundred (no=200) respondents was drawn. However, a total of fifty-six (no=56) responses were found to be incomplete and thus excluded. A total of one hundred and fourteen (no=144) completed questionnaire constitute the analysis of this study.

After the data was collected, a set of rigorous processes were carried out to organize and code the data in a coding book. This process was followed by input of data using excel word sheet and then transported to the SPSS (version 22) statistical package for further analysis. Results of the study are presented using descriptive statistics, graphs, and charts that illustrate the results found in the study. Descriptive statistics were conducted to illustrate some of the findings. To proof the research hypothesis, a multiple linear regression was conducted using statistical tables, graphs, etc.

Out of all the total respondents of hundred and forty-four (no=144), eighty-eight (61.1%) are Men and fifty-six (38.9%) are Women who participated in the online survey. Majority of the respondents that participated in the survey were within the age group of 25-34 (33.3%) years old and those above 40 years old were (5.6%) of the total respondents. Majority of the respondents representing were those who obtained a bachelor’s degree (48.6%); Diploma (24.3%) and master’s degree (14.6%). However, respondents with the lowest level of education are High school graduates (2.5%).

<table>
<thead>
<tr>
<th>TABLE 2: SAMPLING PROFILE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile Category</td>
</tr>
<tr>
<td>Male</td>
</tr>
<tr>
<td>Female</td>
</tr>
<tr>
<td>Age</td>
</tr>
<tr>
<td>18-24</td>
</tr>
<tr>
<td>25-34</td>
</tr>
<tr>
<td>35-49</td>
</tr>
<tr>
<td>Above 40</td>
</tr>
<tr>
<td>Education</td>
</tr>
<tr>
<td>High School</td>
</tr>
<tr>
<td>Diploma</td>
</tr>
<tr>
<td>Bachelor</td>
</tr>
<tr>
<td>Master</td>
</tr>
<tr>
<td>Usage (E-banking services)</td>
</tr>
<tr>
<td>Yes</td>
</tr>
<tr>
<td>No</td>
</tr>
<tr>
<td>Impressions</td>
</tr>
<tr>
<td>Very bad</td>
</tr>
<tr>
<td>Bad</td>
</tr>
<tr>
<td>Neutral</td>
</tr>
<tr>
<td>Good</td>
</tr>
<tr>
<td>Very good</td>
</tr>
</tbody>
</table>

Meanwhile, majority of the respondents are keen users of e-banking or online banking services (72.2%) with a lesser staggering per cent of (27.1%) those that reported that they are not using online banking services. Among all these respondents, we found both positive and negative impressions about e-banking services. Those who evaluated “neutral” concerning their perception of e-banking represent (35.4%). A combined value of (58.3 %) represents those with positive perceptions on e-banking represent those respondents that may currently be satisfied with e-banking services offered by their choice of a bank in The Gambia. Finally, the following part below is the data analysis of the results found in the study, providing further details in the results found.

B. Explanatory analysis of reliability and dimensionality

The study uses five-point Likert’s scale to elicit consumer opinion of e-banking services according to four critical factors. The scales range from strongly disagree to strongly agree. Of all the total respondents, results show that there exist deferring opinions in their evaluation of e-banking factors in this study. The statistical mean (m) for perceived trust (m=3.236), perceived privacy (m=3.0944), perceived security (m=3.7153) and perceived risk (m=2.9635) with a standard deviation of (1.03089), (1.04579), (1.01667) and (0.83675) respectively. These results indicate that respondents are more inclined towards “strongly agree” tendencies (ranging from 0.2 to 0.4) on the scale.

However, we found no responses towards “neutral” or “strongly disagree” tendencies in the result. Meanwhile, perceived security (m=3.7153) has a much bigger evaluation compared to the rest of the measurement scales with a and a standard deviation (1.01667), while perceived risk (m=2.9635) was evaluated the least with a standard deviation (0.83675). This could mean that first, consumers tend to be more concerned about the perceived security while maintaining least concerns about perceived risks. Secondly, the way the question is been framed may have induced such responses in the study due to a lack of understanding of the questions asked. The table below illustrates the descriptive statistics of the constructs used in this study.

<table>
<thead>
<tr>
<th>TABLE 3 A SUMMARY OF MEASUREMENT CONSTRUCTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Statistics</td>
</tr>
<tr>
<td>---------------------------------------------</td>
</tr>
<tr>
<td>No. Valid</td>
</tr>
<tr>
<td>No. Missing</td>
</tr>
<tr>
<td>Mean</td>
</tr>
<tr>
<td>Median</td>
</tr>
<tr>
<td>Mode</td>
</tr>
<tr>
<td>Std. Deviation</td>
</tr>
</tbody>
</table>

C. Descriptive statistics of Gender and constructs

A crosstab statistic observes the relationship between respondents’ gender and their trust in the adoption of e-banking services. Summary of Levene’s test shows that there is a significant difference in consumer evaluation of “perceived privacy” (t=−2.000, sig. = 0.045) showing that females are more susceptible to “privacy concerns” (m=3.3107) in their e-banking transactions compared to their male counterparts (m=2.9568). Our results do not show any enough data to support further the gender difference in the evaluation of e-banking factors as shown in the table below. Finally, of all the other constructs, consumers do not show any significant difference in their evaluation of perceived trust (sig. = 0.34), perceived security (sig. = 0.116), and perceived risk (sig. = 0.188).

<table>
<thead>
<tr>
<th>TABLE 4 DESCRIPTIVE STATISTICS OF GENDER AND CONSTRUCTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Constructs</td>
</tr>
<tr>
<td>---------------------------------------------</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Perceived Trust</td>
</tr>
<tr>
<td>Perceived Privacy</td>
</tr>
<tr>
<td>Perceived Security</td>
</tr>
<tr>
<td>Perceived Risk</td>
</tr>
</tbody>
</table>

D. Findings

Following several studies [e.g. 22], this study uses multiple regression to ascertain the degree of impact of a list of independent factors (such as perceived risk, perceived security and perceived privacy) on a dependent variable (i.e. perceived trust). We test the hypotheses of the study on three independent variables and their impact on the
dependent variable. Before the test of multivariate regression, just like a common practice, we check for multicollinearity issues in the model. Results output on the correlation table below first show that a correlation exists between all testable variables (at least with a weak acceptable level of 0.48). Secondly, we further validate this test using scores in the collinearity statistics. This test confirms that all variables in the model have an acceptable tolerant score of more than 0.1. Furthermore, a test of normality confirms that all the variables used in the model have met the condition of normality. Result emphasis that normality is clear despite an insignificant deviation away from the distribution. It is, however, assumed that this will bear no significant effect on the result of this study.

Results of the multiple linear regression confirm that collectively, all the sets of predictor variables (independent variables) such as perceived risk, perceived security, and perceived privacy have a significant impact on a model outcome (perceived trust) with approximately 0.67 ($R^2 = 67\%)$ of the model fit (where $p$-value < 0.05). Therefore, this model is a good predictor of the outcome found in the study.

The effect of individual predictor variables using $t$-statistics in the model were significant, for example, perceived privacy has a positive impact ($t = 6.428$, sig. = 0.000) on consumer trust. This signifies that consumer evaluation of online banking according to their perceived privacy has a bigger impact on their level of perceived trust in their adoption of e-banking services. Also, consumer evaluation of perceived security associated with online banking transaction have a positive effect on their trust in adopting e-banking services ($t = 3.512$, sig. = 0.001). The standardized coefficients Beta in the evaluation of the impact of each predictor variables (independent variable) on the outcome (perceived trust) showed that only perceived privacy ($\beta = 0.477$) and perceived security ($\beta = 0.268$) account for significant impact on the outcome variable of perceived trust (constant, 0.621) in the model. However, perceived risk ($\beta = 0.048$) accounted for a no significant impact on the model (sig. > 0.05).

The purpose of this study was to identify the key factors that influence the level of perceived security and privacy and their relationship with the level of perceived trust in the adoption of e-banking services. The study also aimed to test the impact of perceived risk on this relationship. As such, we were able to confirm the variables of perceived privacy (H2) and perceived security (H1) as the main drivers affecting consumer trust in the adoption of e-banking services. However, perceived online risk (H3) could not be supported in this study. Studies [e.g. 37] suggest that the intentions to patronize online banking is dependent on the bank’s ability to evoke trust. This is confirmed by the results of our study.

Generally, customer trust has dominated studies on e-commerce business [17]. In fact, in the e-banking front, instilling customer trust should be a priority for banks. For example, Chu et al., [8] emphasize the importance of the consumer engagement and relationship, especially in their adoption and use of e-banking. Thus, customer trust in e-banking arena may depend on their perception of image of the bank [5] online transactions and the conduct online transactions [see 7].

According to the findings, to reduce consumers fears due to high security and privacy concerns, banks must instill confidence by guaranteeing high-security systems, data protection, and flexible, and useable IT systems [26]. These mechanisms would promote consumer confidence in e-banking services. About 35\% of our respondents reported that they are neither impressed nor satisfied with their current e-banking services. Transaction risk associated with e-banking has not been confirmed by study. This result is consistent with the findings of other scholars [e.g. 12].

Further, perceived security is a significant factor influencing consumers’ acceptance of e-banking services. This means when customers develop positive perceptions of security and trust in the use of e-banking is promoted [26]. This result is consistent with similar findings in the literature [e.g. 30; 6; 36]. Consumers feel safe and assured that their financial and personal data would be protected. Therefore, it is imperative for financial institutions to strengthen online security systems and protection of personal and financial identities of their users at all time [1]. Our result is in line with the findings of previous studies [e.g. 12].

The consumer privacy concern is a major factor that influences consumers' willingness to accept e-banking, and this result is confirmed by previous studies [e.g., 20; 23 Yousafzai et al., 2005; 27]. Higher privacy concerns negatively impact customer decision to engage in online transactions which includes e-banking [23, 24]. Thus, banks must adopt more robust privacy policies. Privacy and data protection have been the center of discussions in the field of e-commerce. Meanwhile, e-banking customers continue to raise concerns about the protection of the information they give out to banks. However, consumers’ privacy continues...
to face even greater vulnerability due to the Cookies technology. Bornschein et al., [3] provides an illustrative way that Cookies track consumers’ online activities on corporate websites. The Cookies technology aggregates the consumer online traffic, track consumer clicks on a website, adjust products/service offerings or advertising users’ online activities through various targeting strategies [3]. E-banking providers must be ahead of the emerging cookies technologies to mitigate loss of private data and thus withering consumer online trust. 

B. Conclusion

Financial institutions must recognize customers’ susceptibility to e-banking services. E-banking is a growing phenomenon in the global financial industry that allows for effective customer relationship, relevant information and enabling digital financial transactions. The banks have a responsibility to ensure the usability of the corporate website [9] and recognizing consumer online privacy concerns [34]. This would allow the design of digital applications that enable users’ online experience, satisfaction and positive WoM. However, the growth of cyber risk, identity theft, unauthorized disclosure of private data (Yousafzai et al. 2009; 24) has raised significant challenges in the adoption of e-banking.

To promote users’ trust in online business (e.g., e-banking), EU’s General Data Protection regulation guide online content providers, such as financial institutions to address website content development: (1) a website must provide visible notice about the private user information it collects on its users; and (2) a website must give users a choice to agree/accept and to disagree/rejects to online activity tracking. Considering this, data protection must be increasingly prioritized by banks. Moreover, consumer perceived privacy concerns address the information being collected on consumers and how the information is used. Therefore, the bank must address users’ consent and knowledge of accessing personal and financial information. According to Sheehan and Hoy (2000) US Federal Trade Commission addresses the online privacy and users’ security concerns through five principles of e-commerce content, and thus help safeguard online content users. These principles are applicable to e-commerce environment (i.e. e-banking):

1. Notice: Online consumers should be given notice of an entity’s information practices.
2. Choice: Consumers should be given choice concerning the use and dissemination of information collected from or about them.
3. Access: Consumers should be given access to information about them collected and stored by an entity.
4. Security: Data collectors should take appropriate steps to ensure the security and integrity of information collected.
5. Redress: Enforcement mechanisms, through self-regulation, government regulation, or other means, should be available to ensure compliance.

Future research could observe the role of content messaging and communication to influence customer perception of e-banking services. It is imperative that message and the relevance of online content is are critical elements of consumer awareness and trust about e-banking [8]. Financial institutions must recognize these critical elements of e-banking business, especially the strengthened online security of user financial information [9] and data management must be on top of banks’ e-banking strategy. Also, future research could examine how digital platforms such as websites and mobile application could strengthen the level of engagement, information content, and efficiency of online financial transactions. These are crucial elements confronting the adoption of e-banking services.

The study has recognized a few limitations. This empirical study is constrained by the sampling size which thus limits the generalization of findings. Subsequent studies should consider more robust measurement scales to broaden the scope of the investigation.

Acknowledgement

Special thanks to the anonymous peer-reviewers for their suggestions to improve the content of this research from its original version.

Declaration of Conflicting Interests

The authors declared no potential conflicts of interest concerning the research, authorship, and/or publication of this article.

Funding

The authors received no financial support for the research, authorship, and/or publication of this article.

REFERENCES


DOI: http://dx.doi.org/10.24018/ejbmr.2020.5.2.286


[27] Oreku, G.S. & Li, J. (2005) “Rethinking E-commerce Security” CIMGA-IWAITC (0/05)


