Jibril, Abdul Bashiru; Kwarteng, Michael Adu; Botchway, Raphael Kwaku; Bode, Jürgen; Chovancová, Miloslava

Article

The impact of online identity theft on customers' willingness to engage in e-banking transaction in Ghana: A technology threat avoidance theory

Cogent Business & Management

Provided in Cooperation with:
Taylor & Francis Group

Suggested Citation: Jibril, Abdul Bashiru; Kwarteng, Michael Adu; Botchway, Raphael Kwaku; Bode, Jürgen; Chovancová, Miloslava (2020) : The impact of online identity theft on customers' willingness to engage in e-banking transaction in Ghana: A technology threat avoidance theory, Cogent Business & Management, ISSN 2331-1975, Taylor & Francis, Abingdon, Vol. 7, Iss. 1, pp. 1-22, https://doi.org/10.1080/23311975.2020.1832825

This Version is available at:
https://hdl.handle.net/10419/244984

Cogent Business & Management

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/oabm20

The impact of online identity theft on customers' willingness to engage in e-banking transaction in Ghana: A technology threat avoidance theory

Abdul Bashiru Jibril, Michael Adu Kwarteng, Raphael Kwaku Botchway, Jürgen Bode & Miloslava Chovancova |

To cite this article: Abdul Bashiru Jibril, Michael Adu Kwarteng, Raphael Kwaku Botchway, Jürgen Bode & Miloslava Chovancova | (2020) The impact of online identity theft on customers' willingness to engage in e-banking transaction in Ghana: A technology threat avoidance theory, Cogent Business & Management, 7:1, 1832825, DOI: 10.1080/23311975.2020.1832825

To link to this article: https://doi.org/10.1080/23311975.2020.1832825

Published online: 19 Oct 2020.

Jibril et al., *Cogent Business & Management* (2020), 7: 1832825
https://doi.org/10.1080/23311975.2020.1832825

cogent business & management

MARKETING | RESEARCH ARTICLE

The impact of online identity theft on customers' willingness to engage in e-banking transaction in Ghana: A technology threat avoidance theory

Abdul Bashiru Jibril[1]*, Michael Adu Kwarteng[1], Raphael Kwaku Botchway[2], Jürgen Bode[3] and Miloslava Chovancova[1]

Received: 15 April 2020
Accepted: 29 September 2020

*Corresponding author: Abdul Bashiru Jibril, Department of Management and Marketing, Faculty of Management and Economics, Tomas Bata University in Zlin, Zlin 76001, Czech Republic
E-mail: jibril@utb.cz, mallam-bash13@gmail.com

Reviewing editor:
Len Tiu Wright, De Montfort University Faculty of Business and Law, Leicester, UK

Additional information is available at the end of the article

Abstract: Until recently, studies regarding e-banking transactions have focused more on motivational factors that trigger the intention to accept and use the e-banking transaction, rather than the de-motivational factors that propel the action. However, in the developing countries like Sub-Sahara economies, the factors associated with the former have not been explored and are still rudimentary in the literature. Drawing from the Technology Threat Avoidance Theory (TTAT), the study seeks to examine the impact of online identity theft on customers' willingness to engage in e-banking transactions in Ghana. A quantitative survey of 393 valid responses from retail bank customers amongst two leading commercial banks in Ghana for the analyses. Results from the PLS-SEM showed that the research constructs; perceived online identity theft' positively and significantly predict "fear of

Abdul Bashiru Jibril

Jürgen Bode

ABOUT THE AUTHORS

Ing. Abdul Bashiru Jibril is a Doctoral Researcher at the Department of Management and Marketing at TBU in Zlin. He is particularly interested in deploying data mining techniques in extracting intelligence to improve business decision-making especially for marketers. He has several scientific publications to his credit.

Dr. Michael Adu Kwarteng is a Senior Lecturer at the Department of Management and Marketing, FAME, TBU in Zlin. His research focuses on Digital Marketing and Social media analytics.

Raphael Kwaku Botchway is a Ph.D. candidate with a research interest in Soft Computing, Social Media, and Text Analytics at the Faculty of Applied Informatics, TBU in Zlin, Czech Republic.

Prof. Jürgen Bode is a Full Professor at the Department of Management Sciences at Hochschule Bonn-Rhein-Sieg University of Applied Sciences, Bonn, Germany. His research spans Entrepreneurship and SME's development in the developing countries.

Prof. Miloslava Chovancová *is* an Associate Professor at the Department of Management and Marketing. Her research focuses on Consumer behaviour, Brand management, and SME's development.

PUBLIC INTEREST STATEMENT

Considering the present era of the technology revolution, no industry in today's business world is untouched to the use of Information communication systems (ICT) and for that matter, the banking industry is no exception. This study therefore primarily concentrates on impediments, specifically, the "online identity theft" that obstructs the adoption/engagement of online banking transactions within the purview of a developing country setting, precisely, Ghana (sub-Sahara African region). Despite the growing discussion of electronic banking service adoption in the literature, an insufficient attempt has been made to examine the customers' constraints towards intention to engage in e-banking transactions within the context of an emerging economy (Ghana), Africa. This paper aims to discover consumers' constraints (online identity theft) regarding their inability to engage successfully in e-banking transaction in Ghana given the perspective of ICT. The study offers practical knowledge to banks and other industry players to understand the nature and characteristics of online banking transactions that are best suited for marketing strategies.

financial loss", "fear of reputational damage", and "security and privacy concern" whilst the former has a negative mediated-relationship between perceived online identity theft and the intention to engage in e-banking transaction. This study is the first of its kind that has extended the application of the TTAT framework into the study of e-banking transactions. The study serves as a practical tool that will enable the banks in their quest to assess customers' restriction/aversion towards the use of Fintech while ensuring sustainable growth of e-banking transactions in an emerging economy context. The study is limited to only banking institutions in Ghana without considering other players in the financial sub-sector. Future research direction has been suggested in the concluding part of the paper.

Subjects: Marketing Research; Internet / Digital Marketing / e-Marketing; Retail Marketing

Keywords: Online identity theft; e-banking transaction; technology threat avoidance theory; bank customers; Sub-Saharan Africa; developing country; Ghana

1. Introduction

Over the years, scholars have pursued to test concepts and theories geared towards online consumer research, specifically in line with the acceptance/adoption and rejection of a particular product/service while proffering marketing strategies for such scenarios (Dennis et al., 2009; Jibril, Kwarteng, Chovancova et al., 2020; Wright et al., 2019). Most of these online consumer researches are specifically tailored at e-banking transactions from both developed and developing economies (Jibril, Kwarteng, Nwaiwu et al., 2020; López-Nicolás et al., 2008). It cannot be gainsaid that the outcome of these findings has helped deepen the collective understanding of how financial institutions (banks) and customers perceive the significance of online or e-banking transactions. More often than not, however, these researches present a limited perspective on e-banking transactions with the notion of looking at the motivational factors that trigger the intention to accept and use of the e-banking services (Gyeltshen & Beri, 2019; Hartono et al., 2014; Tarhini et al., 2016) while ignoring the de-motivation factors (avoidance motivations) towards e-banking transactions. The contribution this article makes is to empirically test a theoretical framework bent on eliciting the notion of online identity theft on bank customers' intent to engage in e-banking transactions via the mediating role of online security and privacy concerns; within an emerging country's context (Ghana). This research expands the theoretical discourse of the discipline of digital marketing and offers significant practical welfares as well as managerial implications for the banking sector in developing or emerging economies, arguing that the internet has come to stay and it is not living in extinction within the foreseeable future.

This study argues that, given the rate of internet penetration and diffusion in the market arena, the effect of customer initiation in adopting online transactions over the web may be significant to the banking sector, and that, some aversion to adopting the technology may therefore offer and explain how customers perceive online banking in a lower penetration internet community where this study is domiciled (Oertzen & Odekerken-Schröder, 2019; Pozo et al., 2019). Moreover, this research may help considerably to form a better picture of the research progress in this field. This study investigates the indirect effect of online identity theft as a penchant to engage in online banking transactions via the mediating role of online security and privacy concerns within an emerging country's context. However, the perception of cybersecurity threat and its effect on online transactions remain a major setback particularly, for consumers of e-product and e-services (Kimani et al., 2019). This perception, from the extant literature, includes; fear of financial loss, and fear of reputational damage, and other related security and privacy concern. Meanwhile, the banking sector in the 21st century is poised to increase its customer loyalty and attract new customers as the primary drivers associated with the use of internet banking platforms (Mishra, 2005). Hence, a calibre of this study can help to validate other theoretical models, add value to

existing theories, and may go a long way to assist or redefine new theories/models within the online adoption and retention theories. The study augments the theorization of the acceptance or threats effects in engaging in online transactions in the banking sector by eliciting other variables which are key to acceptance or rejection of the online transactions and subsequently offering pragmatic solutions to that effect.

In the financial sector, perceived online identity theft is noted to be characterized by vulnerable transactions in which internet banking systems cannot be isolated, due to the harmful impact, such as; confidentiality, integrity, and privacy of a bank and its customers (Hille et al., 2015; Jibril, Kwarteng, Nwaiwu et al., 2020; Jordan et al., 2018; Nwaiwu et al., 2020). In the existing literature, however, two important issues that appear to have derailed and received insufficient investigations regarding aversion/impediment of the customer regarding the engagement of online banking transactions emerge, specifically in the unindustrialized economy: First, within the empirical research domain, few studies have analysed perceived online identity theft (POIT) towards the tendency for a customer to initiate online transactions, even though works of Polasik and Wisniewski; and Hille, Walsh, and Cleveland (Hille et al., 2015; Polasik & Piotr Wisniewski, 2009) made use of this construct in their study, it was not narrowed to the e-banking transactions and also not directed at the sub-Saharan African context that this study proposes and contributes to the literature; and second, this study accordingly seeks to access the influence of perceived online identity theft on the penchant of a customer to engage in online banking transactions. This assessment will highlight on the customers' preparedness to generally assess online banking transactions via the mediating role of security and privacy concerns (SEPCON) while giving a better understanding to FinTech operators.

Although it is imperative to note that customer perception of "online identity theft" may indeed influence the tendency for the customer to engage/disengage in the action, while there could be varied outcomes that might be recorded in our empirical findings, specifically geared towards the demotivation tendencies considering the perception formed out of this displeasure (thus, online identity theft) which potentially interferes (Rheingold, 1991) with bank customer's decision process regarding the e-banking adoption (or engagement) and retention, and hence heeds the call for an empirical inquiry. To sum up, the goals of this research is to: *(1) the consequences of online identity theft on customers intention to engage in ebanking transaction; and (2) examine the mediation role security and privacy concern on the attraction between online identity theft and the intention to engage in ebanking transaction*. Hence, the study serves as a wake-up call into the practical retention of customers in the e-banking fraternity and also as a reminder to the business organization's survival regarding its customer base (retention). Findings of this paper would propel the financial institutions to strategically strengthen their security and privacy concern since cybercrime (online identity theft) instances in the banking sector is concerned.

The paper subsequently begins with the state of ICT in the banking sector of Ghana, a theoretical foundation that spans bank marketing, adoption of information communication technology and leads to the proposed research model, as well as complementary research hypotheses. Followed by the methodology section which details the data collection procedure. The next, results, followed by general discussion and research implications. Finally, the paper concludes with limitations and future research directions.

2. The state of information technology (IT) in the banking sector of Ghana

There is quite a slow pace with regards to the adoption of electronic banking (e-banking) in developing countries, particularly in Sub-Saharan Africa (Boateng et al., 2008). Meanwhile, the Information and communications technologies (ICTs) have persistently reformed the way and manner in conducting business transactions and satisfying the growing demands of customers for most organizations. Globally, it is quite to note that the potential of ICTs applications in the banking sector has been seen in terms of its capacity to increase customer base, reduce transaction costs (cost-effectiveness), improve the quality and timeliness of response, enhance opportunities for advertising and branding, facilitate self-service and service customization, improve

customer communication and relationship among others (Boateng et al., 2016; Nabareseh et al., 2014). Interestingly, in recent times, banks in developed, and some in developing parts of the world offering e-banking services are with various levels of complexity (Woldie et al., 2008). However, most banks in Africa seemed to be content with having a relatively few Web presence of them making steps towards fully completed e-banking integration.

In Ghana, a frantic effort has been made by the government and private firms to catch up with global developments regarding the improvement of the quality of service delivery across both local and international banks in the Ghanaian banking industry. Instances can be seen where some banks have allowed some form of internet-related transaction for their clients via their new banking system, checking their account balances, and to deposit/transfer money from one account to another (Boateng et al., 2016; Woldie et al., 2008). Over the past two decades, the Ghanaian banking industry has witnessed a gradual and continual application/integration of computerized technology into banking operations. Again, the application ICT since the past two decades has become a core strategic tool for competitive advantage by redefining market segmentation as well as market share so far as e-banking adoption is concerned. At present, there is a massive influx of ICT of various forms into several banking operations in Ghana. These include (1) computerization of counter processes and banking operations—all banks; (2) national network of all or key branches across the country, (3) introduction of Automated Teller Machines (ATMs), (4) creation of smart cards, and debit cards, (5) introduction of personal banking facilities (telephone banking, SMS banking, and on-line virtual terminals), (6) introduction of Internet banking, etc (Jibril, Kwarteng, Pilik et al., 2020; Ofori et al., 2017).

Research over the years has dealt with various aspects of the concept of fraud, cybersecurity, phishing, online identity thefts among others associated with online banking transactions. (Jibril, Kwarteng, Chovancova et al., 2020; Tyagi, 2019) Undeniably, the Internet, therefore, is considered as wild cyberspace, an arena for commercialization, consumerism, business, and leisure, among others. Yet, the phenomenon has become more common in digital-related transactions such as telecoms and financial sectors. Despite persistent advantages accompanying ICT, the concepts; online identity theft, and security and privacy concerns play a significant role concerning the intention to adopt and use technology/innovation (Kimani et al., 2019; Tyagi, 2019). In light of this, the growing knowledge of the concept; perceived online identity theft (POIT) is regarded as a driver that could potentially trigger the varied perception of customers towards the acceptance and retention of new technology. Similarly, in the minds of every ICT user (such as e-shopper, e-bank customer, etc.), the underlying concept; POIT in the research theme denotes the consequences (negative effect) regarding the use of ICT which consequently transcend to the user's decision/intention of the technology.

More importantly, banking in Ghana has undergone many changes in service delivery to improve the quality of service being provided to the customers. These banks, in general, were serving their customers through the manual system which is characterised with long queues to embark on any financial transaction. Though, with the advent of ICT in the banking system, the other problem faced by banking institutions in Ghana in the wake of internet banking is that many clients are unable to engage successfully with the new system. Some of the problems (constraints) are associated with socioeconomic factors in which this study seeks to highlight despite other relevant factors.

2.1. Theoretical foundation: technology threat avoidance theory (TTAT)

Unwillingness to embark on internet-related transactions amongst a large number of beneficiaries (customers) in developing economies remains under-explored in the literature. The present study, therefore, lensed through the Technology Threat Avoidance Theory (TTAT) pioneered by Liang and Xue (Liang & Xue, 2009), to augment the ongoing debate on why individuals or organizations may feel reluctant to accept or engage in a new technology/innovation. The theory asserts that individuals' perceptions regarding their susceptibility (vulnerability) to and the resulting severity

of technology threats influence their awareness of the threats, which, in turn, influences their motivation and behaviour to avoid them.

In the information technology (IT) realm, TTAT suggests that the way that users perceive a threat influences their motivation to invoke a safeguarding mechanism against it. Liang and Xue (Liang & Xue, 2010) tested their theory verifying the theoretical underpinnings and offering their model to explain technology threat avoidance behaviour. The original model of TTAT includes perceptions of susceptibility, severity, threat, safeguard effectiveness, safeguard costs, self-efficacy, avoidance motivation, and avoidance behaviour (Carpenter et al., 2019). The information society in the 21st century is rapidly changing the overall paradigm of business and society as well as the socio-economic environment of individuals about the development of the internet and information & telecommunications technology (ICT).

To take inspiration from TTAT, it is quite remarkable to note that most of technology or information system studies have been conducted around the technology acceptance theory. Though it is imperative to consider the factors determining the acceptance ICT. However, acceptance behaviour may not be regarded as the only dimension in using ICT. The attitude of trying to avoid the use of ICT may be a part of that human behaviour. Therefore, it would be quite meaningful to investigate the use of ICT threat-avoidance behaviour within the confines of internet banking in a developing country. Fundamentally, the avoidance and acceptance behaviours are two different dimensions/perspectives and this makes the technology acceptance theory not complete when the threat-avoidance behaviour of users is silent. Though there are few studies related to the technology threat, while TTAT has expanded the theory by blending various references in the fields of psychology, health care, risk analysis, and information system. Therefore, to understand the behaviour of ICT users who tries to avoid online identity theft, Liang and Xue (2009) proposed the technology threat avoidance theory (TTAT). They argue that TTAT as a dynamic and positive feedback loop could explain about the avoidance behaviour through the cybernetic theory and coping theory. To this, if users/potential are aware of possible theft and consider it seriously as a negative result, they will perceive it as a technology threat. Similarly, the threat awareness may draw a coping judgment and users may evaluate/assume the level that the technology threat can be avoided through unwillingness to engage in the e-banking platform. Therefore, we argue in the present study that the validity of TTAT starts with the assumption that the avoidance and acceptance behaviours of people are different from the qualitative perspective and hence must be looked at.

The overall e-banking literature gives credence to the significance associated with the benefits gained for the customer, the trade merchants, and the banking institutions alike (Al-Somali et al., 2009; Sharma, 2011; Wan et al., 2005). A cross-country research authored by Nyangosi et al., (2009) in two developing or emerging economies revealed that customers in both countries have developed a positive attitude and hence attach much prominence to the emergence of e-banking in this technological era. Indeed, Botchway et al. (2020) opined that e-banking enables banks to offer low cost and high value-added financial services to their clients. Again, the works of Hasan (2002) and Gikandi & Bloor, (2010) attest to the fact that online banking has erupted as a significant strategy for financial institutions, in general, to attract and preserve their valued customers. Considering the overall perspectives of the importance of e-banking to the banks in general, Sharma (2011), states that, the banking institutions stand to gain in these three ways (*1) E-banking websites can act as a revenue earner through its promotional activities to the banking firm (2) Customers can avail e-banking facility from anywhere, therefore saving the need not to invest more on building infrastructures and (3) Websites that offer financial convergence for the customer will create a more involved banking customer who will more frequently utilize the banking websites*. All these circumstances presuppose that the enactment of e-banking transactions enables the banking institutions or firms to outwit their competitors and hence gain revenue. The term online or e-banking here refers to "a method of banking in which transactions are conducted electronically over the Internet". Online banking (e-banking), on the other hand, enables bank customers to handle account management and perform account transactions directly with the bank through the internet. This, however, comes with its purported benefits and

challenges to the customer as well as the banking institution itself. One such challenge is connected with privacy and security issues which have been established in the literature (Fernandes et al., 2014; Miyazaki & Fernandez, 2001). Besides, a survey conducted by the online banking association, cited in the works of Mishra (Mishra, 2005), indicated that member institutions of the association rated security as the most pertinent concern or issue associated with e-banking transactions. Hence, unwillingness on the part of a bank customer to engage in the internet banking platform for a successful and easier financial transaction remains a major concern amongst several financial institutions even given the purported benefit to the interest of the banks as a whole as earlier stipulated.

2.2. Conceptual model and hypothesis development

To begin with, the researchers developed a conceptual model, as well as the summary of research constructs and definition with their literature sourced, are given in Figure 1 and Table 1 respectively.

2.2.1. The link between perceived online identity theft (POIT), fear of financial loss (FOFL), security and privacy concern (SEPCON), and customer intention (INTENT) to engage in e-banking transaction

Perceived identity theft is described as one of the several dimensions of cyber-security threats. This occurs when the individual is perceived that his/her identity (such as name, address, mobile number, etc.) could be stolen by the third party in a transaction regarding any related e-business Lai, Li, and Hsieh, (Lai et al., 2012). This is because, the proliferation of online business transactions has led to a huge number of incidents of identity theft, which have gained expensive costs to consumers and e-commerce industries in a larger perspective. This presupposes that combating identity theft is important for both online businesses and consumers (Fernandes et al., 2014). Therefore, it worth noting that the practical significance of fighting identity theft has been of great interest to scholars in the marketing filed, yet limited research has been done in this scope.

Studies by Boateng et al. (2016), concerns about privacy protection is one of the primary obstacles for consumers to participate in electronic Commerce transactions that require them to divulge personal information, such as their date of birth, social security number, personal phone number, credit card information among others. This makes the protection of consumers' privacy as an important factor for the success of e-commerce businesses. This view is also supported by Martín, Camarero, & José (Martín et al., 2011) who in their research focused on online shoppers in Portugal, explored the effect of trust on perceived benefits of online purchase, by looking at how security and privacy considerations of the internet-related transactions in Portugal influenced their trust levels and confidence to use the system. They found a causal relationship between users' perceptions of risk and their decision to trust the system, which ultimately influenced their purchase intentions along with the perceived benefits of using the system. In light of this, we extend the scope of our study to capture the behaviour of bank customers regarding the inability

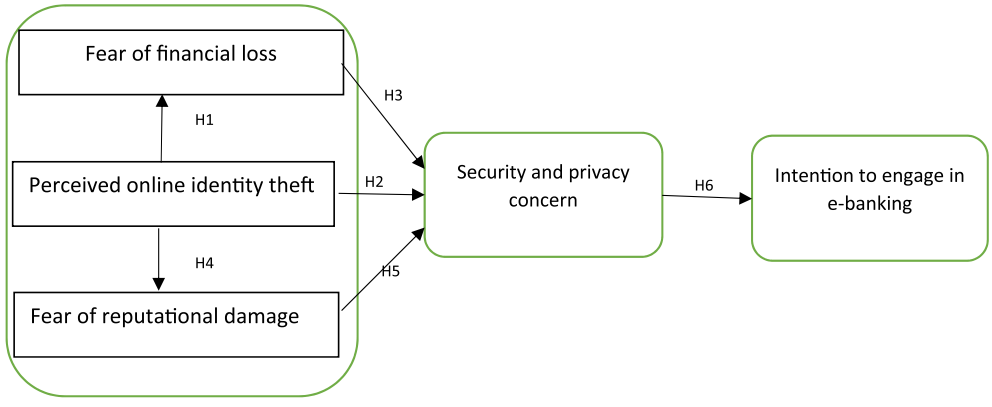

Figure 1. Research model.
Source: Authors' own.

Table 1. Constructs, definition, and their sources

S/N	Construct	Definition	Literature adopted
1	Fear of financial loss (FOFL)	*Loss in psychology refers to the emotional side of investing, namely the negative sentiment associated with recognizing a loss and its psychological effects.* *It also refers to the tendency that new technology in the banking space causes harm to investors or depositors.* *The fear of financial losses dimension is defined as the fear of illegal or unethical appropriation and usage of personal and financial data by a cyber-criminal or other entity to gain financial benefits such as buying products on behalf of the victim*	Hille et al., 2015)
2	Fear of reputational damage (FORD)	*Reputational risk is a threat to the positive perception others have or should have about an individual, company, products or services.*	Hille et al., 2015)
3	Security and privacy concern (SEPCON)	*Internet privacy involves the right or mandate of personal privacy concerning the storing, provision to third parties, and displaying information about oneself via the Internet. Internet privacy is a subset of data privacy. Privacy concerns have been articulated from the beginnings of large-scale computer sharing.*	(Hille et al., 2015)
4	Perceived online identity theft (POIT)	*Identity theft, also known as identity fraud, is a crime in which an imposter obtains key pieces of personally identifiable information, such as Social Security or driver's license numbers, to impersonate someone else.* *Online identity theft is a serious crime, often aimed at obtaining the personal or financial information of another person. The obtained information is then used for personal gain, often by making purchases or selling someone's identity or credit card details online to the highest bidder*	(Eisenmann, 2006; Jibril, Kwarteng, Nwaiwu et al., 2020; Walsh et al., 2016)
5	Intention to engage in e-banking	*The intention is a mental state that represents a commitment to carrying out an action or actions in the future. Intention involves mental activities such as planning and forethought.*	(Ajzen, 1991; Jibril, Kwarteng, Nwaiwu et al., 2020)

to engage and the internet banking platform for financial transactions. To understand the empirical antecedent to the concept (INTENT) as the overall dependent variable concerning POIT, the following hypotheses are proposed as a basis to investigate the causal relationship between FOFL and bank customers' willingness to engage in the online banking transaction. Also, this will be done by investigating the mediating effect (if any) of online security vis-à-vis privacy concerns. Hence, we state that;

H1: Perceived online identity theft (POIT) positively predict fear of financial loss (FOFL) regarding e-banking transaction.

H2: Perceived online identity theft (POIT) positively predict online security and privacy concern (SEPCON) regarding e-banking transaction.

H3: FOFL positively mediates the relationship between POIT and SEPCON in the quest to engage in e-banking transactions.

2.2.2. The link between perceived online identity theft (POIT), fear of reputational damage, online security and privacy concern (SEPCON), and customer intention (INTENT) to engage in e-banking transactions

The perception of online identity theft has been deeply characterised in several internet-related transactions including financial institutions. Despite the unprecedented benefits accompanied by the use of internet communication technology (ICT), the consumer(s) patronage via online shopping medium continues to increase, while there are still doubts and restraining factors that impact on the consumers' behavioural intentions and willingness to use such systems. These doubts and restraining factors (avoidance motivations) including stolen personal details; such as name, account details, password/pin code among others, are some unpleasant factors that potentially resit many users of ICT especially in the financial sub-sector of a developing country (Jibril, Kwarteng, Chovancova et al., 2020; Jibril, Kwarteng, Pilik et al., 2020). Again, several banks and non-banking institutions face the same challenges when it comes to financial transactions using the internet banking platforms (Hartono et al., 2014). Some of these factors bother on issues such as the fear of reputational damage that is connected to online security and privacy concerns held by consumers (Hille et al., 2015). As part of scientific inquiry that aims to investigate the relationships between FORD and issues such as perceived risk associated (security and privacy concern) toward the intentions to embark on online transactions from the consumers' perspective, results from the research conducted by San Martín, Camarero, & San José (Martín et al., 2011) showed that there is a direct positive relationship between POIT and FORD by taking into consideration SEPCON. This study collaborated the research of (Jibril, Kwarteng, Nwaiwu et al., 2020) which was conducted within the context of understanding the impact of fear of identity theft and perceived risk on the Online Purchase Intention of consumers. This is in tandem with the works by other researchers who have investigated related issues (Gurung & Raja, 2016). Consequently, this research further aims to investigate specifically, how POIT and FORD influence online consumers' intent to engage in e-banking transaction by further considering the mediating role of SEPCON on POIT and INTENT towards customer engagement in e-banking transactions in Ghana. Hence, we proposed the hypotheses that;

H4: Perceived online identity theft (POIT) positively predict fear of reputation damage (FORD) in the e-banking transaction.

H5: SEPCON positively mediates the relationship between FORD and INTENT in the quest to engage in e-banking transactions.

H6: Customer's SEPCON negatively affect the intention to engage in e-banking transaction.

3. Materials and methods

This study is purely a quantitative inquiry. It takes inspirations by deducing (adapting) research constructs from the constructs dimension of the existing Technology Threat Avoidance Theory (TTAT) by Liang and Xue (2009).

3.1. Sampling design and data collection

The study deployed both randomize and non-randomize sampling techniques for data extraction. First, with the non-randomized sampling technique (non-probability), we adopted it for the selection of our target banks (unit of analysis. It was necessary because our target banks were scattered all over the major 10 administrative regions of Ghana, hence this technique (precisely convenient sampling technique) (Goodman, 1961; Madow, 1968). The technique was noted among these criteria which include among others—accessibility, geographical proximity, willingness to participate,

participants' accessibility to the researcher, and affordability in terms of cost (Etikan et al., 2016). In line with these reasons, we considered two leading commercial banks who have integrated online banking services in their routine operation (notably, GCB bank and Ecobank Limited) in Ghana for the survey. Secondly, after selecting the target banks, the randomized sampling technique was applied. With this probability sampling technique, each customer of these selected banks is given the equal chance to be selected for the study irrespective of whether he/she is off-line or on-line bank customer.

Data were finally collected through the intercept approach and online survey by a structured questionnaire. By intercept, we mean customers were trapped/intercepted at the bank's premises while the online survey link was sent to participants who requested it mainly because they were not ready and also not having much time to attend to the survey at that particular time duration. Out of the 450 questionnaires distributed, 393 were eligible for analysis. Survey respondents were pre-qualified to ensure that their knowledge of online banking services, as well as its accompanying online theft issues, was adequate to answer the survey questions. Data collection was undertaken in the months between January to March 2020. On average, the questionnaire took 7 min to fill. Findings show the majority (70%) of the respondents are university educated (bachelor, Master's, and PhD degrees). Previous studies have shown that technology/innovation adopters are mainly educated relative to the uneducated population (Nwaiwu et al., 2020; Tarhini et al., 2016). Therefore, in this study, it is obvious that the researchers considered most of the study participants from a university education background, since these participants (university educated) are the future players of technology acceptance/usage and sustainability especially in developing countries and particularly, Ghana, and the sub-Sahara Africa in general. Again, regarding the study theme, it would be quite necessary to consider more people who are at least in higher education since they may constitute the upper class who would have adequate knowledge of the subject matter, hence our decision to consider such a percentage of study participants (sample). Table 2 below depicts a socio-demographic profile of respondents for this study.

3.2. Constructs measurement

The research constructs and their sources have been presented in Table 1. The items were measured on a Likert scale using; 1-Completely disagree, 2—disagree, 3—neutral,—agree, and 5—Completely agree. It is important to note that, the research constructs were adopted from the literature while the instruments/items used in measuring the constructs were adapted from the extant literature to suit the current study, and are shown in a subsequent table (see Table 4: factor loadings).

3.3. Test of common method bias (CMB)

Taking inspiration from Podsakoff (Podsakoff, 2003), the authors stated in the present survey questionnaire particularly in the header section that there are no right or wrong answers to the questions asked. We further assured our respondents of their anonymity and also informed them that they were free to quit filling the questionnaire at any time. Moreover, as earlier stated, different anchors were employed in the questionnaire. Besides the qualitative measures taken to address potential concerns about CMB, this study, following the recent suggestions in the PLS-SEM literature and particularly Kock & Hadaya (Kock & Hadaya, 2018), we employ the full collinearity approach, specifically variance inflation factor (VIF) for detecting evidence on CMB. The results of this post-hoc measure indicate that CMB is not a key concern since the computed VIFs are less than three (3) considering the maximum threshold of five (5). Again, following previous research (Jibril, Kwarteng, Pilik et al., 2020), the current work concludes that since a study that examines the presence of mediation effect, it is extremely difficult for respondents themselves to mentally manipulate. Therefore, the concerns about CMB are minimal here, hence in this analysis, the potential for CMB is low.

4. Results

The test of the research model relied on Partial least square and structural equation modelling (PLS-SEM) in ADANCO 2.0 Version.

Table 2. Summary of socio-demographic characteristics of respondents

Details of respondents		Frequency	Percent (%)
Gender	Male	232	59.0
	Female	161	41.0
Age	18–25	41	10.4
	26–30	133	33.8
	31 – 35	140	35.6
	36–40	55	14.0
	Above 40	24	6.1
Educational level	Basic School (Primary School)	0	0
	Secondary (High) School	90	23.0
	Bachelor's/ Undergraduate	163	41.5
	Master's	95	24.6
	PhD	15	3.8
	Others	30	7.6
Citizenship status	Ghanaian	369	93.9
	A foreign resident in Ghana	24	6.1
Online visitation	Yes	345	87.8
	No	48	12.2
Use of online banking service	Yes	197	50.1
	No	196	49.9
The medium of internet access	Own Laptop	130	33.1
	Home/Personal PC	41	10.4
	School/Office PC	56	14.2
	Smartphone/Mobile Phone	143	3.6
	Cybercafé PC	23	5.9
The frequency internet use	Daily	265	67.4
	Weekly	61	15.5
	Once or twice in a month	25	6.4
	Once or twice in 3 months	10	2.5
	Few times in a year	16	4.1
	Never	6	1.5
Respondents' location	Accra metropolitan:	145	39.9
	GCB Bank Ltd.	90	22.9
	Ecobank Ghana	55	14.0
	Kumasi metropolitan:	141	35.9
	GCB Bank Ltd.	78	19.8
	Ecobank Ghana	63	16.0
	Sunyani Municipal:	107	27.2
	GCB Bank Ltd.	56	14.2
	Ecobank Ghana	51	13.0
	Total (N)	393	100.0

Source: Field survey, January—March 2020 in Ghana.

Table 3. Construct reliability and validity

Construct	Dijkstra-Henseler's rho (ρA)	Jöreskog's rho (ρc)	The average variance extracted (AVE)	Cronbach's alpha(α)
Fear of financial loss	0.8883	0.9215	0.7464	0.8854
Security & privacy concern	0.9149	0.9458	0.8533	0.9140
Fear of reputation damage	0.9265	0.9426	0.8044	0.9188
Intention to engage	0.9312	0.9198	0.6992	0.9006
Online identity theft	0.8783	0.9225	0.7992	0.8730

Source: Authors' processing from Adanco 2.1 version

4.1. Model fittest

To begin with, it worthwhile to accord with the recommendations in the PLS-SEM literature (J. J. Hair et al., 2017), the constructs' reliabilities were checked using Dijkstra-Henseler's rho along with Cronbach's alpha coefficients. As shown in Table 3, all the values exceeded the cut-off values of 0.5 indicating strong coefficients of construct's reliability as suggested by Bagozzi and Yi 1988; Hair et al. (2014). The software ADANCO 2.0 (Dijkstra & Henseler, 2015) was used to evaluate the psychometric properties of the constructs and their underlying items. Using the Jöreskog's rho (pc), composite reliability, with a threshold of 0.8. The composite reliability (CR) of the research construct is presented by Dijkstra-Henseler's rho (ρA) with a minimum reliability coefficient 0.8883 and a maximum of 0.9301, while convergent validity was presented by average variance extracted (AVE) which also exceeded the minimum threshold of 0.5 (see Table 3). Regarding discriminant validity, well-known Fornell-Lacker's criteria (Fornell & Larcker, 1981) was used to establish discriminant validity among the latent variables (Henseler et al., 2015). Results from Fornell-Lacker's criterion indicated that constructs satisfy both basic and stringent assumptions and this, therefore, establishes discriminant validity. It worth noting that the coefficients in the diagonal (in bold) of the Fornell-Lacker's table (see Table 5) indicate AVE's of the measured constructs and must greater than 0.5. At the same time, each construct's AVE should be of higher value (coefficient) at both column and row position over other constructs so that discriminant validity could be established.

Moreover, with regards to the indicator loadings of the latent constructs, all items were loaded meaningfully and satisfactory to their corresponding construct measured. The measured indicators have minimum loadings (coefficients) of 0.6755 and maximum loadings of 0.9353 showing a high factor loading. According to Bagozzi and Yi (1988), a loading above a threshold of 0.6 is the best measurement of a latent variable under study since it measures what it ought to measure in practice. Hence, the summary of all the research constructs as well as their measurement items (indicators) is shown in Table 4 with their corresponding loadings (coefficients).

4.2. Structural equation modelling—hypothesis testing

After the assessment of the model is established, the structural model (path analysis) of the hypothetical examination is necessary. Also, it is imperative to achieve this stage of the analysis since it identifies and establishes the effect of the construct relationships of the underlying research constructs. The evidence of our analysis shows that perceived online identity theft (POIT) has both direct and indirect effects (relationship) towards the intention to engage in e-banking transactions. The direct effects describe the straight paths (antecedent variables) towards the dependent variable (intention to engage in ebanking), whilst the indirect effects explain the role of the mediator variable (security and privacy concern) regarding the interaction between the antecedents and the dependent variable.

Table 4. Indicator (Factor) loadings

Construct	*Indicator*	Loadings
Fear of financial loss	*FOFL1: I am afraid that somebody could steal my money while I am transferring my personal data online.*	0.7770
	FOFL2: I am scared that a criminal could use my credit card account number to do online shopping in my name.	0.9029
	FOFL3: I am frightened that somebody could do online shopping at my expense	0.8976
	FOFL4: I am worried about an unauthorized person making online purchases using my personal data	0.8725
Fear of reputation damage	*FORD1: FORD1: I am frightened of somebody using my personal data on the Internet in order to run me down.*	0.8521
	FORD2: I am very worried that the unauthorized use of my personal data online could damage my reputation.	0.9146
	FORD3: I am worried about my reputation being damaged due to the illegal use of my personal data online.	0.9256
	FORD4: The thought that a stranger could damage my reputation by using my personal data online scares me.	0.8934
Security and privacy concern	*SEPCON1: I don't think the Internet has got enough safeguards to make me feel comfortable using it to transact personal business.*	0.9195
	SEPCON2: I don't feel assured that legal and technological structures adequately protect me from problems on the Internet.	0.9353
	SEPCON3: I don't feel confident that encryption and other technological advances on the Internet make it safe for me to do business/transaction there.	0.9164
Perceived online identity theft	*POIT1: I am scared that when I have to give my credit card number to shop online that it could be misused.*	0.9125
	POIT2: I am scared that when I have to give my bank account number to shop online that it could be misused.	0.9323
	POIT3: I am scared that my bank account could be hacked by an unknown person.	0.8340
Intention to engage	*INTENT1: I would use Internet banking for purchasing a product/service.*	0.9042
	INTENT2: I would always consider using the Internet for my shopping.	0.8735
	INTENT3: Given the chance, I would try to buy items online via internet banking.	0.9274
	INTENT4: In the future, I will most likely be using Internet banking for payments.	0.7734
	INTENT5: Using Internet banking for transfer/deposit is something I would do.	0.6755

Source: Authors' processing from Adanco 2.1 version.

4.2.1. Direct effect

The results from the hypothetical path (H1, H2, and H4) show that POIT has a direct (positive) and significant relationship with customers' fear of financial loss (FOFL), fear or reputation damage (FORD), and security and privacy concern (SEPCON) by (β = 0.3871, t = 5.1684), (β = 0.3198, t = 3.5114), and (β = 0.2811, t = 3.8915) respectively (see Table 6), all the hypotheses were supported. The path coefficient is presented by beta (β) and the significant level of each coefficient is presented by the t-test (t-value) of bootstrapping results of 1000 random samples. Again, FOFL also has a direct effect toward SEPCON with (β = 0.3450, t = 4.4506), FORD has a direct effect

Table 5. Test/evidence of discriminant validity—Fornell–Lacker Criterion

Construct	1	2	3	4	5
	FOFL	**SEPCON**	**FORD**	**INTENT**	**POIT**
Fear of financial loss	0.7465				
Security & privacy concern	0.3467	0.8533			
Fear of reputation damage	0.3747	0.3714	0.8044		
Intention to engage	0.0618	0.0179	0.0416	0.6990	
Perceived online identity theft	0.1498	0.2458	0.1023	0.0010	0.7992

Note: Squared correlations; AVE in the diagonal (in bold). Source: Authors' processing from Adanco 2.1 version.

toward SEPCON with (β = 0.3982, t = 5.1684), while SEPCON consequently has a negative and statistically insignificant relationship toward INTENT by (β = −0.1339 t = −1.0273). Meanwhile, it is important to note that, for any construct coefficient to be statistically significant in this research, we considered the threshold of t-value (t > 1.96) which is equal to a p-value (P < 0.05). Therefore, concerning the analysis of the direct relationship, only the link between SEPCON and INTENT path has a negative and insignificant effect from the statistical point of view (see Table 6).

4.2.2. Indirect effect (mediation analysis)

Our partial least square and structural equation modelling (PLS-SEM) reveals three indirect relationships amongst the underlying research construct, notably H3, H5, and H6. This analysis indicates a mediating role of a specific construct(s) regarding a partial impact it has on a relationship between a dependent and independent variable. A careful look into our analysis shows that FOFL, FORD, and SEPCON performed a mediating role as far as the relationship between POIT and INTENT is concerned (see Figure 2). The result, however, shows that both "fear of financial loss (β = −0.0345) and fear of reputation damage (β = −0.0484)" constructs have a negative (but indirect) relationship via the construct 'security and privacy concern' towards customers' intention to engage in e-banking transactions. Though the construct 'perceived online identity theft' has an indirect (but positive) and significant relationship toward SEPCON (dependent variable) by (β = 0.2155, t = 3.9655) through both FOFL and FORD (independent variables), at the same time it (POIT) consequently maintains a negative indirect relationship toward INTENT (β = −0.0664, t = −0.9265), suggesting a statistically insignificant relationship (see Table 6). We, therefore, conclude that the indirect or mediated hypotheses (H3, H5, and H6) were supported per our statistical estimations (see the estimated model in Figure 2).

4.2.3. Coefficient of determination (r)

Regarding the measurement of the predictive power known as the coefficient of determination (R^2) of the regression model. The coefficient indicates the percentage of variation in the dependent variable that is been explained by the predictor (independent) variable (Hair et al., 2019). In the same vein, the Adjusted R^2 shows the amount of variance in the endogenous construct explained by the exogenous constructs. From Table 6, the estimated R^2 of FOFL (0.1504) showed 15% of the variation in the construct FOFL (as a dependent) is explained by the construct POIT (as an independent). Again, the R^2 of FORD (0.1017) showed a 10% variation in the construct FORD is explained by the construct POIT. Whilst model R^2 of SEPCON (0.5121) indicates the total variation of the construct SEPCON explained by the combined effect of individual constructs; FOFL, FORD, and POIT, and these estimates could be traced in Table 6 below. Also, the dependent variable INTENT with R^2 = 0.279 shows that 27.9% of the variation in the construct INTENT is explained by the predictor variable SEPCON. Additionally, the authors a goodness-of-fit test to measure how well the observed data correspond to the fitted (assumed) model (see Table 6 for the estimates).

Table 6. Path coefficient; Direct and Indirect relationship

Effect	Original coefficient (β)	Standard bootstrap results					Empirical remarks
		Mean value	Standard error	t-value	p-value (2-sided)	p-value (1-sided)	
Direct effect:							
Fear of financial loss -> Security & privacy concern	0.3450	0.3476	0.0775	4.4506	0.0000	0.0000	Supported
Security & privacy concern -> Intention to engage	−0.1339	−0.1351	0.1303	−1.0273	0.3045	0.1523	Not Supported
Fear of reputation damage -> Security & privacy concern	0.3982	0.3966	0.0789	5.0483	0.0000	0.0000	Supported
Perceived online identity theft -> Fear of financial loss	0.3871	0.3946	0.0749	5.1684	0.0000	0.0000	Supported
Perceived online identity theft -> Fear of reputation damage	0.3198	0.3259	0.0911	3.5114	0.0005	0.0002	Supported
Perceived online identity theft -> Security & privacy concern	0.2811	0.2783	0.0722	3.8915	0.0001	0.0001	Supported
Indirect effect:							
Fear of financial loss -> Intention to engage	−0.0345	−0.0477	0.0483	−0.9566	0.3390	0.1695	Not Supported
Fear of reputation damage -> Intention to engage	−0.0484	−0.0543	0.0537	−0.9921	0.3214	0.1607	Not Supported
Online identity theft -> Security & privacy concern	0.2155	0.2700	0.0658	3.9655	0.0001	0.0000	Supported
Online identity theft -> Intention to engage	−0.0664	−0.0390	0.0377	−0.9265	0.3544	0.1772	Not Supported
Dependent variable:	Coefficient of determination (R^2)			Adjusted R^2			
Fear of financial loss	0.1504			0.1451			-
Security & privacy concern	0.5121			0.5029			-
Fear of reputation damage	0.1017			0.0961			-

(*Continued*)

Table 6. (*Continued*)

Effect	Original coefficient (β)	Standard bootstrap results					Empirical remarks
		Mean value	Standard error	t-value	p-value (2-sided)	p-value (1-sided)	
Intention to engage	0.2790			0.2018			-
Goodness of model fit							
	Value			HI95			HI99
SRMR	0.0640			0.1070			0.1652
dULS	0.7794			2.1744			5.1853
dG	0.6018			0.7679			1.2472

Note: β = regression coefficient and t = significant value (t > 1.96) or (P < 0.05)

Source: Authors' processing from ADANCO 2.1 Version

cogent business & management

cogent business & management

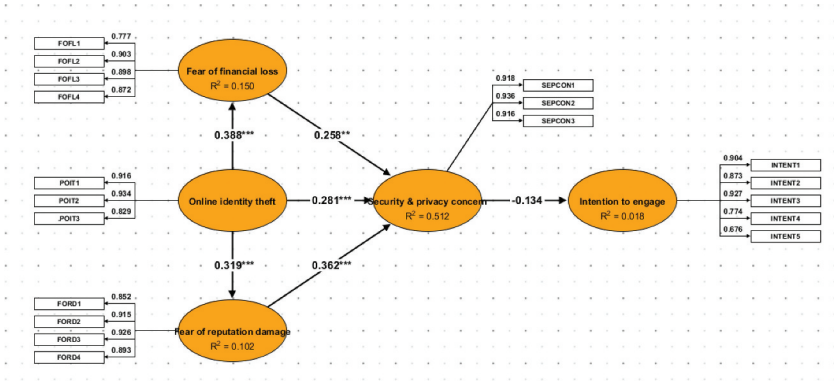

Figure 2. Estimated research model Source: Authors' processing from ADANCO 2.0.1.

5. General discussion

It is important to acknowledge the fact that the information society in the 21st century is rapidly changing the overall paradigm of business and society as well as the socio-economic environment of individuals about the development of internet and information & telecommunications technology. Today, this development is creating an enormous value in the domestic and global economy which can be manifested from industries as they are rapidly diffused throughout the industries such as distribution, finance, auction, entertainment, delivery service among others. Concerning financial businesses, the information technology (IT) is not an issue of selection but the general trend that cannot go against for the sake of its survival. In simple terms, this suggests that the perception of online identity theft in the literature can be a fatal threat to the business unable to use IT while it can also be a great opportunity to the business of using IT appropriately. Similarly, considering the large change (innovation brought about by the internet and IT, the entire society and individuals and businesses have tried hard to adopt and use IT to adapt to this change.

The intention to accept a new technology especially in the developing countries continues to dominate in the ongoing debate so far as technology acceptance and usage are concerned. A careful look into our finding shows that demotivational factors from security and privacy perspective continue to be a stumbling-block (challenge) amongst under-developed economic settings. Owing to this, the aforementioned constructs in this study (fear of financial loss, fear of reputation damage, online identity theft, and security and privacy concern) are noted and could be described as 'avoidance motivation' (Hille et al., 2015). This is because perception formed out of these concepts consequently triggers customer's behavioural intention toward the use of a particular product/service. Inferring from the works of Amegbe and Osakwe (Amegbe & Osakwe, 2018; Uduma et al., 2015) concerning customer loyalty, it has become prudent for bankers to shore up their momentum to attract more customers since the era of competitiveness in the banking sector is invoked within the developing nations, despite the multiple institutional voids and lower level of infrastructural conditions in these developing nations.

The study further suggests that since a customer may perceive that his/her identity could be stolen by a third party, he/she may feel reluctant to engage in such a 'risky transaction'. At the same time, since the customer anticipates that his/her identity could be stolen in the event of e-banking transactions, the resultant outcomes could be expressed as a fear of financial loss and fear of reputation damage as seen from our research model (see Figure 1). For example, a customer is afraid that somebody could steal his/her money while transferring his/her personal data online. He/she may be scared that a criminal could use his/her credit card account number to do online shopping in his/her name. Additionally, perceived online identity theft, as well as privacy and security concern constructs, continue to be a huge hindrance to amongst customers of banks in a developing country like Ghana since e-banking transaction is concerned. Perceive. For instance, a customer may be worried about an unauthorized person making online purchases using his/her

data. Also, he/she may be worried that the unauthorized use of his/her data online could damage his/her reputation, and this consequently corroborated with the works of Fernandes et al. 2014; Walsh et al. 2016; Wu et al. (2014) regarding the menace of perceived online identity theft.

The study further establishes that; customers are unwilling to engage in e-banking transactions mainly because they think the internet has not got enough safeguards to make them feel comfortable by using it to transact personal business. Notwithstanding, they (bank customers) in an underdeveloped country in Africa, like Ghana, do not feel assured that legal and technological structures adequately protect them from problems on the Internet and are also not feeling confident that encryption and other technological advances on the Internet make it safer for them to do business/transaction via e-banking services. More so, intention to engage in e-banking from our study revealed that Ghanaians though would like to use this innovation (internet banking), but are scared with regards to security and privacy concerns they have in mind. This perceived cue (security and privacy concern) triggers a negative relationship with towards intent to engage in the e-banking transaction amongst the survey customers.

Again, it worth noting that the study addresses whether there is a direct relationship amongst constructs: fear of financial loss, fear of reputation damage, and security and privacy concern in an event of online identity theft towards intent to engage in e-banking transactions in Ghana, a developing country. With the consensus of online identity theft in an emerging country, this study does shed more light, by considering the scenario in an emerging economy. Hence, the present findings are in line with the study of Jibril et al. 2020; Walsh et al. (2016), and a shred of further evidence from Walsh, Hille, and Cleveland, (Walsh et al., 2016) stated that personal and financial data can have a dire lasting financial consequence for victims and does incur a negative financial credit rating for such victims and this claim supported our present study. Adding to this claim by Mitchison and co, the present study does expound the tendency that fear of financial loss will predict or affect the customers' decision to engage in e-banking transactions in an emerging economy. Again, with the research works of Jordan et al. (2018) regarding the indirect effect of fear of financial loss and fear of reputation damage relative to the INTENT, their study turned out to have positive relationships that contradict our current study even though their work was not situated in a developing context. Adding to this debate is the findings that emanated from the multiple research works of Hille et al, (Hille et al., 2015; Rhoa & Yub, 2011) stating that fear of financial loss and fear of reputation damage has a positive and significant effect on security and privacy concern than INTENT whiles our present study confirmed this claim by reporting that the two constructs (fear of financial loss and fear of reputation damage) have no positive or direct relations with INTENT.

Again, the study addresses whether there is an influence on the mediating role of security and privacy concerns towards INTENT to engage in e-banking service in a developing economy context. Concerning the earlier hypothesis stated, the authors examined that security and privacy concern though, plays a mediating role between perceived online identity theft, fear of financial loss, fear of reputation damage, and INTENT but a negative relationship and statistically insignificant at randomized bootstrapping of T-test ($t > 1.96$). Nonetheless, the positive or direct link between perceived online identity theft and security and privacy concerns per our research estimate was mediated significantly by constructs fear of financial loss and fear of reputation damage, and this ultimately establishes support for our hypothetical relationships (See Table 6). This finding, though largely studied under different contexts in literature, mirrors with previous research works in the risk concerning electronic commerce (e-commerce). With this said, we opine that more research works in the emerging context is required to be performed to address the issue of security and privacy concerns and online identity theft (avoidance motivation) as a conduit towards intent to engage in online-related transactions.

5.1. Research implications

Theoretically, this study is incontestably a pioneering inquiry into the customer's constraints towards online banking transactions in Ghana. In that, the present study will assist in the development of

a scientifically validated conceptual model with regards to internet banking engagement. The theoretical contributions are particularly relevant because most of the research currently available on the subject is largely concentrated on the motivational factors of technology adoption. Again, lack of rigorous scientific validations of the proposed framework within the scope of an emerging economy's context like Ghana, a sub-Sahara African region, would be relevant since the current study ascertain the demotivating factors particularly "avoidance motivation" of technology adoption and retention, specifically, geared toward online banking transaction in a Sub-Sahara African region. Therefore, this research will fill the gap from a theoretical point of view.

Internet banking (technology adoption) has received remarkable attention from scholars and other industry players alike. Online banking transactions have noted in the literature to be a substantial tool or platform that increases performance with regards to the effectiveness and efficiency of the new technology. Therefore, this study would open a pathway into a more rigorous academic inquiry into other regarding the strategic implementation of digital technologies adoption and engagement in business and society, especially in the banking sub-sector in the banking sector as a subject area of interest. This is particularly interesting considering that a vast majority of research efforts into the subject of digital transformation have remained largely on the motivation factors of new technology adoption. Also, the proposed study would be a wake-up call to scholars and offer them the hidden dimension's customers' constraints that impede the successful engagement of online banking transactions in the developing economy. Hence, it is hoped that this study will in its use of quantitative methods be a guide that would serve as a platform for other researchers to leverage in their scientific inquiry into the phenomenon of customers' constraints towards online banking engagement and other related subjects.

Practically, the study will contribute a practical knowledge through the development of a robust and scientifically validated framework/model that would be useful for practitioners and organizations wishing to embark on the engagement of online transaction-related initiatives within their organizations. The framework will also serve as a practical tool that will enable the organizations especially banks in their quest to assess its level of digital penetration and diffusion while evaluating the impact of the digital revolution on organizational processes to identify firms' successes and failures regarding the application of digital technology. More so, this study would help bankers and other policymakers in the financial industry to strategically deal with the enumerated constraints associated with customers' intention to engage in the online banking transaction.

6. Conclusion

Although the adoption of electronic/online banking, generally referred to as e-banking, and the motivational factors leading to it has received considerable research attention to the neglect of the perceived constraints (avoidance motivations). This research gap, particularly in the Sub-Sahara Africa region (Ghana) has had a slow-pace regarding bank customers' intention to engage in e-banking services. Therefore, the study aimed to develop and test a theoretical framework bent on eliciting the notion of online identity theft on bank customers' intent to engage in e-banking transactions via the mediating role of online security and privacy concern; within an emerging country's context. To help banks foster customer's continued usage of their e-banking services and attract potential customers in an emerging economy setting, this study developed and tested a new research model of online identity theft as well as security and privacy concerns in the face of e-banking services in a developing country context. A quantitative study of three-hundred and nighty-three (393) customers from two leading commercial banks (GCB bank limited and Ecobank Ghana limited) in Ghana were examined through the intercept approach. The study explores the relationships of both direct and indirect effects of POIT. The construct "POIT" significantly predicts FOFL, FORD, and SEPCON towards INTENT whiles SEPCON negatively mediated towards the former. More so, this study highlights the differences between online identity theft on one hand and its associated intent to engage in e-banking transactions, on the other hand. While this study can predict customers' in an emerging economy, perceived online identity theft towards their zeal to embark on e-banking

service, specifically using three major constructs, i.e., FOFL, FORD, and SEPCON. This study offered a practical relevance for the banking industry on how best they can strategies and repose confidence in their customer's quest to engage in online banking service, whilst they put measures in place to mitigate the menace/perception of online identity theft issues. In sum, this study provides a strong reference point to continue to broaden the literature in the developing economy so far as online banking transactions are concerned, arguing that the financial technology (Fintech) has come to stay.

6.1. Research limitations and future direction

The study is not without limitations. First, the researchers gathered responses from only customers of the banks while ignoring views from the banker's perspective. Second, the study filtered from the literature with emphasis on online identity theft constructs without considering other relevant factors which could potentially impede the engagement of e-banking transaction in Ghana. Third, the sample size of the study is relatively low regarding the number of retail banks in Ghana, thereby affecting the generalization of the work. The paper, therefore, invites future scholars to consider a study which integrates the perspectives from both individual and organizational level. Additional constructs which deemed relevant are also welcomed in future studies. This research further recommends future researchers to expand the sample size as well as the scope of the study, for instance, a comparative study among two sub-Sahara African countries. This will rather increase reliability and the validity of the research model.

Acknowledgements
This work was supported by the Internal Grant Agency of FaME through TBU in Zlín No. IGA/FaME/2019/008 and IGA/FaME/2020/002 and further supported by the Department of Management Sciences, Hochschule Bonn-Rhein-Sieg University of Applied Sciences, Bonn, Germany. We would like to thank Prof. Boris Popesko (Vice-dean for research and business liaison) and Dr. Bedrich Zimola (vice-dean for strategic projects and promotion), all at Faculty of Management and Economics-TBU in Zlin for their consistency and persistence scholarly advice for this publication. The paper was again supported by the resources of A.I. Lab at the Faculty of Applied Informatics, Tomas Bata University in Zlin (ailab.fai.utb.cz) and Project no. IGA/CebiaTech/2020/001.

Funding
The authors received no direct funding for this research.

Author details
Abdul Bashiru Jibril[1]
E-mail: jibril@utb.cz
ORCID ID: http://orcid.org/0000-0003-4554-0150
Michael Adu Kwarteng[1]
Raphael Kwaku Botchway[2]
Jürgen Bode[3]
Miloslava Chovancova[1]
[1] Department of Management and Marketing, Faculty of Management and Economics, Tomas Bata University in Zlin, Mostni 5139, Zlin 76001, Czech Republic.
[2] Faculty of Applied Informatics, Tomas Bata University in Zlin, Nam. T.G.M 5555, Zlin 76001, Czech Republic.
[3] Department of Management Sciences, Hochschule Bonn-Rhein-Sieg University of Applied Sciences, Grantham-Allee 20, Sankt Augustin, Bonn 53757, Germany.

Conflicts of Interest
The authors declare no conflict of interest of whatsoever.

Citation information
Cite this article as: The impact of online identity theft on customers' willingness to engage in e-banking transaction in Ghana: A technology threat avoidance theory, Abdul Bashiru Jibril, Michael Adu Kwarteng, Raphael Kwaku Botchway, Jürgen Bode & Miloslava Chovancova, *Cogent Business & Management* (2020), 7: 1832825.

References

Ajzen, I. (1991). The theory of planned behaviour. *Organizational Behaviour and Human Decision Processes*, *50* (2), 179–211. *View At*. https://doi.org/10.1016/0749-5978(91)90020-T

Al-Somali, S. A., Gholami, R., & Clegg, B. (2009). An investigation into the acceptance of online banking in Saudi Arabia. *Technovation*, *29*(2), 130–141. https://doi.org/10.1016/j.technovation.2008.07.004

Amegbe, H., & Osakwe, C. N. (2018). Towards achieving strong customer loyalty in the financial services industry: Ghanaian top banks' customers as a test case. *International Journal of Bank Marketing*, *36*(5), 988–1007. https://doi.org/10.1108/IJBM-06-2017-0120

Bagozzi, R. P., & Yi, Y. (1988). On the evaluation of structural equation models. *Journal of the Academy of Marketing Science*, *16*(1), 74–94. https://doi.org/10.1007/BF02723327

Boateng, H., Adam, D. R., Okoe, A. F., & Anning-Dorson, T. (2016). Assessing the determinants of internet banking adoption intentions: A social cognitive theory perspective. *Computers in Human Behavior*, *65*, 468–478. https://doi.org/10.1016/j.chb.2016.09.017

Boateng, R., Heeks, R., Molla, A., & Hinson, R. (2008). E-commerce and socio-economic development: Conceptualizing the link. *Internet Research*, *18*(5), 562–594. https://doi.org/10.1108/10662240810912783

Botchway, R. K., Jibril, A. B., Oplatková, Z. K., & Chovancová, M. (2020). Deductions from a Sub-Saharan African Bank's Tweets: A sentiment analysis approach. *Cogent Economics & Finance, 8*(1), 1776006. https://doi.org/10.1080/23322039.2020

Carpenter, D., Young, D. K., Barrett, P., & McLeod, A. J. (2019). Refining technology threat avoidance theory. *Communications of the Association for Information Systems*, *44*(1), 22. https://doi.org/10.17705/1CAIS.04422

Dennis, C., Merrilees, B., Jayawardhena, C., & Wright, L. T. (2009). E-consumer behaviour. *European Journal of Marketing*, *43*(9/10), 1121–1139. https://doi.org/10.1108/03090560910976393

Dijkstra, T. K., & Henseler, J. (2015). Consistent partial least squares path modeling. *MIS Quarterly*, *39*(2), 297–316. https://doi.org/10.25300/MISQ/2015/39.2.02

Eisenmann, T. R. (2006). Internet companies' growth strategies: Determinants of investment intensity and long-term performance. *Strategic Management Journal*, *27* (12), 1183–1204. https://doi.org/10.1002/smj.567

Etikan, I., Musa, S. A., & Alkassim, R. S. (2016). Comparison of convenience sampling and purposive sampling. *American Journal of Theoretical and Applied Statistics*, *5* (1), 1–4. https://doi.org/10.11648/j.ajtas.20160501.11

Fernandes, D. A. B., Soares, L. F. B., Gomes, J. V., Freire, M. M., & Inácio, P. R. M. (2014). A quick perspective on the current state in cybersecurity. In Babak Akhgar and Hamid R. Arabnia (Eds.), *Emerging trends in ICT security* (pp. 423–442). Elsevier.

Fornell, C., & Larcker, D. F. (1981). *Structural equation models with unobservable variables and measurement error: Algebra and statistics*. SAGE Publications Sage CA.

Gikandi, J. W., & Bloor, C. (2010). Adoption and effectiveness of electronic banking in Kenya. *Electronic commerce research and applications*, *9*(4), 277–282. https://doi.org/10.1016/j.elerap.2009.12.003

Goodman, L. A. (1961). Snowball sampling. In *The annals of mathematical statistics* (pp. 148–170). Institute of Mathematical Statistics.

Gurung, A., & Raja, M. K. (2016). Online privacy and security concerns of consumers. *Information & Computer Security*, *24*(4), 348–371. https://doi.org/10.1108/ICS-05-2015-0020

Gyeltshen, C., & Beri, N. (2019). Levels of work place happiness, organizational commitment, work motivation, and job satisfaction among secondary school teachers in bhutan. *International Journal of Recent Technology and Engineering*, *7*(6), 428–435. http://ijoe.vidyapublications.com/Issues/Vol11/03_Vol.11.pdf

Hair, F. J., Jr, Sarstedt, M., Hopkins, L., & Kuppelwieser, G. V. (2014). Partial least squares structural equation modeling (PLS-SEM) An emerging tool in business research. *European Business Review*, *26*(2), 106–121. https://doi.org/10.1108/EBR-10-2013-0128

Hair, J., Hollingsworth, C. L., Randolph, A. B., & Chong, A. Y. L. (2017). An updated and expanded assessment of PLS-SEM in information systems research. *Industrial Management & Data Systems*, *117*(3), 442–458. https://doi.org/10.1108/IMDS-04-2016-0130

Hair, J. F., Risher, J. J., Sarstedt, M., & Ringle, C. M. (2019). When to use and how to report the results of PLS-SEM. *European Business Review*, *31*(1), 2–24. https://doi.org/10.1108/EBR-11-2018-0203

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

Hasan, Z. (2002). Mudaraba as a mode of finance in Islamic banking: theory, practice and problems. https://mpra.ub.uni-muenchen.de/id/eprint/2951

Henseler, J., Ringle, C. M., & Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. *Journal of the Academy of Marketing Science*, *43*(1), 115–135. https://doi.org/10.1007/s11747-014-0403-8

Hille, P., Walsh, G., & Cleveland, M. (2015). Consumer fear of online identity theft: Scale development and validation. *Journal of Interactive Marketing*, *30*, 1–19. https://doi.org/10.1016/j.intmar.2014.10.001

Jibril, A. B., Kwarteng, M. A., Chovancova, M., & Denanyoh, R. (2020). *Customers' perception of cybersecurity threats toward e-banking adoption and retention: A conceptual study*. ICCWS 2020 15th International Conference on Cyber Warfare and Security, 270. Norfolk, Virginia: Academic Conferences and publishing limited.

Jibril, A. B., Kwarteng, M. A., Nwaiwu, F., Appiah-Nimo, C., Pilik, M., & Chovancova, M. (2020). *Online identity theft on consumer purchase intention: A mediating role of online security and privacy concern*. Conference on E-Business, e-Services and e-Society, 147–158. Skukuza, South Africa: Springer.

Jibril, A. B., Kwarteng, M. A., Pilik, M., Botha, E., & Osakwe, C. N. (2020). Towards understanding the initial adoption of online retail stores in a low internet penetration context: An exploratory work in Ghana. *Sustainability*, *12*(3), 854. https://doi.org/10.3390/su12030854

Jordan, G., Leskovar, R., & Marič, M. (2018). Impact of fear of identity theft and perceived risk on online purchase intention. *Organizacija*, *51*(2), 146–155. https://doi.org/10.2478/orga-2018-0007

Kimani, K., Oduol, V., & Langat, K. (2019). Cyber security challenges for IoT-based smart grid networks. *International Journal of Critical Infrastructure Protection*, *25*, 36–49. https://doi.org/10.1016/j.ijcip.2019.01.001

Kock, N., & Hadaya, P. (2018). Minimum sample size estimation in PLS-SEM: The inverse square root and gamma-exponential methods. *Information Systems Journal*, *28* (1), 227–261. https://doi.org/10.1111/isj.12131

Lai, F., Li, D., & Hsieh, C.-T. (2012). Fighting identity theft: The coping perspective. *Decision Support Systems*, *52* (2), 353–363. https://doi.org/10.1016/j.dss.2011.09.002

Liang, H., & Xue, Y. (2009). Avoidance of information technology threats: A theoretical perspective. In *MIS quarterly* (pp. 71–90). Management Information Systems Research Center, University of Minnesota.

Liang, H., & Xue, Y. (2010). Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the Association for Information Systems*, *11*(7), 394–413. https://doi.org/10.17705/1jais.00232

López-Nicolás, C., Molina-Castillo, F. J., & Bouwman, H. (2008). An assessment of advanced mobile services acceptance: Contributions from TAM and diffusion theory models. *Information & Management*, *45*(6), 359–364. https://doi.org/10.1016/j.im.2008.05.001

Madow, W. G. (1968). *Elementary sampling theory*. Taylor & Francis.

Martín, S. S., Camarero, C., & José, R. S. (2011). Does involvement matter in online shopping satisfaction and trust? *Psychology & Marketing*, *28*(2), 145–167. https://doi.org/10.1002/mar.20384

Mishra, A. K. (2005). Internet banking in India part-I. *International Journal of Marketing Research Vol*, *1*, 186–198.

Miyazaki, A. D., & Fernandez, A. (2001). Consumer perceptions of privacy and security risks for online shopping. *Journal of Consumer affairs*, *35*1, 27–44. https://doi.org/10.1111/j.1745-6606.2001.tb00101.x

Nabareseh, S., Osakwe, C. N., Klímek, P., & Chovancová, M. (2014). A comparative study of consumers' readiness for internet shopping in two African emerging economies: Some preliminary findings. *Mediterranean Journal of Social Sciences 5*(23). https://doi.org/10.5901/mjss.2014.v5n23p1882

Nwaiwu, F., Kwarteng, M. A., Jibril, A. B., Buřita, L., & Pilik, M. (2020). *Impact of security and trust as factors that influence the adoption and use of digital technologies that generate, collect and transmit user data*. ICCWS 2020 15th International Conference on

Cyber Warfare and Security, 363. Norfolk, Virginia: Academic Conferences and publishing limited.

Nyangosi, R., Arora, J. S., & Singh, S. (2009). The evolution of e-banking: a study of Indian and Kenyan technology awareness. *International Journal of electronic finance*, *3* (2), 149–165. https://doi.org/10.1504/IJEF.2009.026357

Oertzen, A.-S., & Odekerken-Schröder, G. (2019). Achieving continued usage in online banking: A post-adoption study. *International Journal of Bank Marketing*, *37*(6), 1394–1418. https://doi.org/10.1108/IJBM-09-2018-0239

Ofori, K. S., Boateng, H., Okoe, A. F., & Gvozdanovic, I. (2017). Examining customers' continuance intentions towards internet banking usage. *Marketing Intelligence & Planning*, *35*(6), 756–773. https://doi.org/10.1108/MIP-11-2016-0214

Podsakoff, N. P. (2003). Common method biases in behavioral research: A critical review of the literature and recommended remedies. *Journal of Applied Psychology*, *885*(879), 10–1037. https://psycnet.apa.org/buy/2003-08045-010

Polasik, M., & Piotr Wisniewski, T. (2009). Empirical analysis of internet banking adoption in Poland. *International Journal of Bank Marketing*, *27*(1), 32–52. https://doi.org/10.1108/02652320910928227

Pozo, H., Akabane, G. K., & Tachizava, T. (2019). Innovation and technology processes in micro and small business. *Cogent Business & Management*, *6*(1), 1588088. https://doi.org/10.1080/23311975.2019.1588088

Rheingold, H. (1991). *Virtual reality: Exploring the brave new technologies of artificial experience and interactive worlds-from cyberspace to teledildonics*. Secker & Warburg.

Rhoa, H., & Yub, I. (2011). *The impact of information technology threat avoidance factors on avoidance behavior of user*. Dep. Bus. Manag. Sunc. Natl. Univ.

Sharma, A. (2011). *Take-off of online marketing: casting the next generation strategies*. Business Strategy Series. https://doi.org/10.1108/17515631111155160

Tarhini, A., El-Masri, M., Ali, M., & Serrano, A. (2016). Extending the UTAUT model to understand the customers' acceptance and use of internet banking in Lebanon: A structural equation modeling approach. *Information Technology & People*, *29*(4), 830–849. https://doi.org/10.1108/ITP-02-2014-0034

Tyagi, S. (2019). *Cybercrime overwhelming online banking: A Project Management approach's alternative1*. PM World Journal. http://www.pmworldjournal.net/.

Uduma, I. A., Wali, A. F., & Wright, L. T. (2015). A quantitative study on the influence of breadth of open innovation on SMEs product-service performance: The moderating effect of type of innovation. *Cogent Business & Management*, *2*(1), 1120421. https://doi.org/10.1080/23311975.2015.1120421

Walsh, G., Hille, P., & Cleveland, M. (2016). *Fearing online identity theft: A segmentation study of online customers*. ECIS, Research-in.

Wan, W. W., Luk, C. L., & Chow, C. W. (2005). Customers' adoption of banking channels in Hong Kong. International Journal of bank marketing. https://doi.org/10.1108/02652320510591711

Woldie, A., Hinson, R., Iddrisu, H., & Boateng, R. (2008). *Internet banking: An initial look at Ghanaian bank consumer perceptions*. Business perspectives.

Wright, L. T., Robin, R., Stone, M., & Aravopoulou, D. E. (2019). Adoption of Big Data technology for innovation in B2B marketing. *Journal of Business-to-Business Marketing*, *26* (3–4), 281–293. https://doi.org/10.1080/1051712X.2019.1611082

Wu, L.-Y., Chen, K.-Y., Chen, P.-Y., & Cheng, S.-L. (2014). Perceived value, transaction cost, and repurchase-intention in online shopping: A relational exchange perspective. *Journal of Business Research*, *67*(1), 2768–2776. https://doi.org/10.1016/j.jbusres.2012.09.007

Cogent Business & Management **(ISSN: 2331-1975) is published by Cogent OA, part of Taylor & Francis Group.**

Publishing with Cogent OA ensures:

- Immediate, universal access to your article on publication
- High visibility and discoverability via the Cogent OA website as well as Taylor & Francis Online
- Download and citation statistics for your article
- Rapid online publication
- Input from, and dialog with, expert editors and editorial boards
- Retention of full copyright of your article
- Guaranteed legacy preservation of your article
- Discounts and waivers for authors in developing regions

Submit your manuscript to a Cogent OA journal at www.CogentOA.com